AUDITORÍA AL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE GESTIÓN DE INCIDENTES DE CLIENTES DE ANS COMUNICACIONES, CON BASE EN LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002

JOSE MIGUEL FUENTES CARO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C MAYO 2019

AUDITORÍA AL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE GESTIÓN DE INCIDENTES DE CLIENTES DE ANS COMUNICACIONES, CON BASE EN LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002

JOSE MIGUEL FUENTES CARO

TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE ESPECIALISTA EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

ASESOR: MENG. JAIRO ALEJANDRO BUITRAGO ROMERO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C MAYO 2019

Nota de Aceptación

_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Firma del Director de Proyecto

Bogotá D.C. Junio de 2019

DEDICATORIA

Dedico este proyecto de grado a todas las personas y entidades que hicieron posible la ejecución no solo del proyecto sino de la base de conocimiento adquirida para el desarrollo del mismo y en especial a mi familia por ser el faro de mi vida.

AGRADECIMIENTOS

Agradezco a mi familia por el apoyo brindado con paciencia y amor. A ANS Comunicaciones por facilitarme los espacios y talento humano para las necesidades del proyecto. A mi tutor, el Ing. Jairo Buitrago por su guía y apoyo para coronar el premio de montaña fuera de categoría. A Cable & Wireless por la motivación dada para mi crecimiento profesional y, por último, pero no menos importante a Dios, porque la fe mueve montañas.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

ANS COMUNICACIONES S.A. es una empresa del sector de las telecomunicaciones que brinda soluciones de conectividad, energía y sistemas inteligentes en varios departamentos de Colombia.

Desde 1999 se ha caracterizado por ser una compañía con cultura corporativa enfocada en la flexibilidad, dinamismo y crecimiento continuo de todas sus áreas, procesos y sub-procesos, proporcionando servicios de alta calidad bajo modalidad de negocio bidireccionalmente rentables.

La gestión de incidentes de clientes es un proceso que ha evolucionado de acuerdo a los requerimientos del negocio enfocándose en atender los requerimientos planteados por las operaciones que se deben ejecutar en los servicios que la compañía presta no solo para brindar el soporte que los servicios requieren sino que se cuente con informaciones que sea confiable, integra y que se encuentre disponible, la cual sirva de base para la toma de decisiones y velar por el cumplimiento de los compromisos contractuales con los clientes.

Este proyecto tiene como finalidad auditar al sistema de gestión de la seguridad de la información del proceso de gestión de incidentes de clientes de Networking de la ANS COMUNICACIONES, bajo las guías dadas por la norma TÉCNICA COLOMBIANA NTC-ISO/IEC 27002.

En la primera parte del proyecto se describirá el proceso de gestión de incidentes de la compañía, con el fin de identificar los requisitos de seguridad de la información y determinar los riesgos a los que está expuesta la seguridad del proceso.

Con base en la guía ISO 27002:2013, se diferenciarán los dominios involucrados en los sistemas de información dentro del proceso para de esta manera seleccionar los controles a evaluar dentro del proceso.

Como resultado de la evaluación, se inferirá las recomendaciones para las mejoras del sistema de gestión de seguridad de la información, las que se darán a la gerencia de ANS COMUNICACIONES. A su vez, se formularán las directrices a desarrollar y finalmente especificar las acciones a implementar dentro del proceso de gestión de incidentes de clientes dentro del marco del sistema de gestión de la seguridad de la información.

El proyecto tendrá como pilar la definición de auditoría que es definida por el portal de ISO 27001 como (Neira, 2012) “El proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.”

1. GENERALIDADES

1.1 Línea de Investigación

SISTEMAS DE INFORMACIÓN

1.2 Planteamiento del problema

El sistema de gestión de la seguridad de la información de los procesos de gestión de incidentes de clientes de ANS Comunicaciones no ha sido auditado, lo que no ha permitido medir el grado de exposición de los activos de información a los riesgos y vulnerabilidades y las acciones necesarias para evitarlos y mitigarlos.

1.2.1 Antecedentes del problema.

ANS COMUNICACIONES ha ampliado su portafolio de servicios no solo a grandes carriers del mercado de telecomunicaciones (como Century Link) sino que en los últimos años amplio su alcance a prestar servicios de red (Internet y VLAN extendida) de manera directa a clientes del sector industrial. ANS COMUNICACIONES basa su portafolio en su infraestructura desplegada en regiones de difícil acceso en nuestra geografía como los llanos orientales, La Guajira, el bajo Cauca, entre otras.

La compañía ha hecho inversiones en aplicaciones para cubrir las diferentes áreas de la operación

y aunque las mismas han cumplido con el propósito para el cual han sido implementadas, no hay certeza de que la seguridad de los sistemas de información esté debidamente implementada para mantener la confidencialidad, integridad y disponibilidad que ella requiere.

1.2.2 Pregunta de investigación.

¿Es posible mediante la auditoría a la seguridad de los sistemas de información de gestión de incidentes de clientes de ANS COMUNICACIONES, desarrollar directrices de seguridad a dicho sistema?

1.2.3 Variables del problema.

A continuación, enunciaré las variables que se encuentran en el planteamiento de problema:

- ✓ Número de hallazgos de auditoría
- ✓ Número de no conformidades.
- ✓ Recomendaciones

1.3 Justificación

La información de disponibilidad es parte del proceso de gestión de Incidentes, el cual sirve de base para las negociaciones de indisponibilidad de servicios. ¿En qué nivel se encuentra la Seguridad, Disponibilidad e integridad de esta información?

Porcentaje de disponibilidad	Monto de penalización
>=99.6%	0% del cargo mensual
Entre >=99% y 99.6%	5% del cargo mensual
Entre >=97% y 99.5%	10% del cargo mensual
Entre >=95% y 97%	20% del cargo mensual
Entre >=90% y 95%	50% del cargo mensual
<90%	100% del cargo mensual

Tabla 1 Tabla de penalización por incumplimiento de Disponibilidad

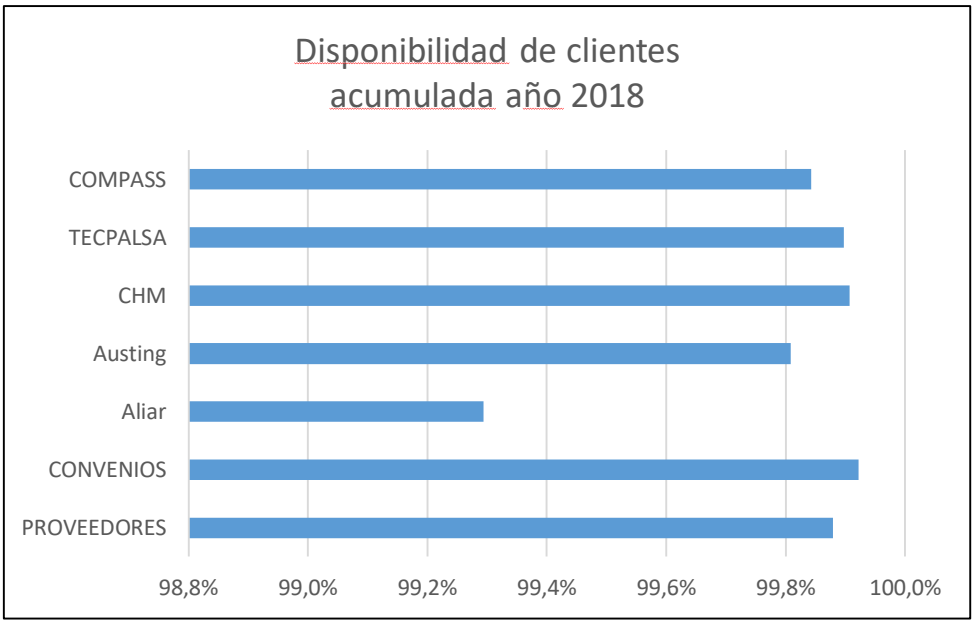
Tomando como base la información proporcionada por el programa OSTicket que en la actualidad brinda los reportes de disponibilidad de cada uno de los clientes y que contiene la siguiente información:

- ✓ Cliente
- ✓ Enlace
- ✓ Ancho de banda
- ✓ Tipo de servicio.
- ✓ Reporte de falla.
- ✓ Medida de tiempos de Disponibilidad
    - o Tiempo de Indisponibilidad (Minutos)
    - o Fecha (dd/mm/aaaa)
    - o Total indisponibilidad
    - o Total disponibilidad

- ✓ Observaciones

Se realizó un cálculo de la disponibilidad acumulada durante el año 2.018 de los clientes de ANS encontrando que uno de sus siete clientes actuales no cumple con la disponibilidad descrita en la tabla 1.

Ilustración 1Disponibililidad de clientes Acumulada año 2.018



Fuente: El Autor

Esto repercute en varios frentes de la compañía:

- ✓ En el financiero porque obliga a la compañía a emitir pagos por multas de indisponibilidad.
- ✓ En el reputacional porque afecta la imagen de la compañía frente a sus clientes.
- ✓ En el recurso humano porque recursos que se pueden invertir en el talento humano se deben invertir en el pago de indisponibilidades.

Durante el año 2.018, ANS COMUNICACIONES debió pagar por concepto de indisponibilidades la suma de $3.145.000, discriminados por cliente en la tabla “Descuentos por indisponibilidad año 2018”:

	CLIENTE						
MES	**CONVENIOS**	**AUSTING**	**CHM**	**ALIAR**	**COMPASS**	**TECPALSA**	**PROVEEDORES**
ENERO	$ 315.000				$ 90.000		
FEBRERO	$ 104.000			$ 547.400			
MARZO	$ 135.000						
ABRIL							
MAYO							
JUNIO	$ 183.050						
JULIO	$ 806.000		$ 340.000				
AGOSTO	$ 342.475						
SEPTIEMBRE							
OCTUBRE							
NOVIEMBRE	$ 220.000	$ 62.475					
DICIEMBRE							
TOTAL POR CLIENTE	$ 2.105.525	$ 62.475	$ 340.000	$ 547.400	$ 90.000	$ -	$ -

Tabla 2 Descuento por indisponibilidad año 2018

ANS Comunicaciones busca tener herramientas para garantizar a sus clientes que la información que usa para mostrar el desempeño de sus servicios sea confiable y basada en la realidad del servicio.

1.4 Objetivos

1.4.1 Objetivo general

Elaborar una auditoría al sistema de gestión de la seguridad de la información del proceso de gestión de Incidentes de clientes de ANS Comunicaciones, con base en la norma ISO 27002:2013.

1.4.2 Objetivos específicos

- ✓ Describir el sistema de información del proceso de gestión de incidentes de ANS Comunicaciones.
- ✓ Identificar los requisitos de seguridad de la información para el proceso de gestión de incidentes de ANS Comunicaciones.
- ✓ Determinar los riesgos de seguridad de la información para el proceso de gestión de incidentes de ANS Comunicaciones.
- ✓ Diferenciar los dominios involucrados en los sistemas de información del proceso de gestión de Incidentes de ANS Comunicaciones, con base en la guía ISO 27002:2013.
- ✓ Seleccionar los controles a evaluar dentro del sistema de información del proceso de gestión de incidentes de ANS Comunicaciones, con base en la guía ISO 27002:2013.
- ✓ Inferir las recomendaciones a dar para las mejoras al sistema de gestión de la seguridad de la información por parte de la Gerencia de Servicios de ANS Comunicaciones.
- ✓ Formular las directrices a desarrollar por parte de ANS Comunicaciones para el sistema de gestión de la seguridad de la información del proceso de gestión de incidentes.
- ✓ Especificar las acciones a implementar por parte de ANS Comunicaciones dentro del proceso de gestión de incidentes de clientes, con base en los resultados de la auditoría al sistema de gestión de la seguridad de la información.

2 MARCOS DE REFERENCIA

2.1 Marco conceptual

Dentro de los procesos de la compañía ANS COMUNICACIONES, la atención de incidentes tiene un papel fundamental. La compañía debe registrar no solo los incidentes que se registran en sus servicios a los clientes, sino que debe hacer seguimiento de los eventos que acontecen en los diferentes componentes de su red CORE.

El proceso de gestión de incidentes está estructurado para recolectar la información necesaria para identificar al cliente que genera el requerimiento, iniciar las labores diagnóstico y determinar las labores que conduzcan a la solución del incidente. Todas las labores deben quedar registradas en la herramienta de seguimiento de casos.

2.1.1 Proceso de gestión de incidentes.

Dentro del proceso para la atención de incidentes se ejecutan las siguientes actividades:

2.1.2.1 Solicitud del cliente.

El cliente realiza la solicitud de servicio al centro de incidentes de ANS COMUNICACIONES. La solicitud puede ser por un comportamiento anómalo del servicio (caída, intermitencias, saturación) o por un requerimiento comercial (altas, bajas, quejas, reclamos).

2.1.2.2 Asignación, coordinador y base.

Dependiendo del tipo de incidente, el mismo es asignado dentro de la herramienta al encargado de turno de la gestión de dicho tipo de incidente. El encargado del incidente realiza las siguientes actividades:

- ✓ Se comunica vía telefónica con la persona que reportó el incidente con base en la información que registro en el ticket.
- ✓ Se valida con la persona del cliente el estado de los equipos y de los componentes de red involucrados en el servicio para determinar las posibles causas del evento.
- ✓ Dependiendo de la revisión, se determina la acción a ejecutar:
    - Cierre del caso.
    - Desplazamiento de personal técnico.
    - Ajustes en la configuración de la red.
    - Notificación a otras áreas.

2.1.2.3 Gestión de permisos.

En caso de que se deba desplazar personal técnico, se realiza con el cliente la coordinación de permisos para ingresar a la localidad afectada. El personal de gestión de incidentes envía vía correo electrónico los datos personales de la persona o personas que atenderán el servicio técnico.

2.1.2.4 Agendamiento de actividad.

Se coordina con el cliente el horario y fecha, así como con el equipo técnico asignado por

parte del área de gestión de incidentes. Este desplazamiento debe estar dado en función de los niveles de servicio acordados con el cliente.

2.1.2.5 Alistamiento técnico.

El personal técnico asignado debe realizar el alistamiento de los equipos de reserva que se tienen asignados para la ejecución de las tareas de mantenimiento. Estos equipos son asignados por el coordinar del área base donde se ubica el servicio afectado. La asignación de equipos depende del reporte dado por el área de gestión de incidentes que recibió el llamado del cliente.

2.1.2.6 Ejecución del servicio.

El personal técnico llega a la ubicación del servicio reportado como afectado. El personal realiza las validaciones técnicas y realizas las reparaciones conducentes al restablecimiento del servicio. Una vez ejecutadas las labores y reestablecidos los servicios, el personal técnico confirma con el cliente la operatividad de sus servicios. Es necesaria la confirmación por parte del cliente para el retiro acordado del personal de la ubicación y confirmación con el área de gestión de incidentes de clientes de la fecha y hora de restablecimientos de los servicios. Una vez el personal técnico diligencia el formato de actividades técnicas, se procede al retiro del personal.

2.1.2.7 Control de calidad y finalización del servicio.

Una vez ejecutada las acciones anteriores, se documenta en el sistema de información lo

ocurrido. Esta acción se debe ejecutar en cada interacción que se haga, tanto con el cliente como interna.

- ✓ Para realizar el cierre del caso, se acuerda con el cliente el tiempo de indisponibilidad del evento en el cual se tiene en cuenta:
  - Hora de reporte del incidente
  - Tipo de falla que causó el incidente
  - Responsable del evento reportado
- ✓ Una vez acordado el tiempo de indisponibilidad, se parametriza el incidente, se documenta el ticket con lo ocurrido en el mismo y se procede al cierre.
- ✓ Al cliente y las áreas de servicio de ANS COMUNICACIONES les es enviado un correo con la notificación del cierre de incidentes con la información mencionada en los puntos anteriores.

2.1.2.8 Entrega, Aprobación y Medición de Satisfacción.

Mensualmente, el personal de servicio al cliente genera desde la plataforma de gestión de incidentes un reporte por cada cliente relacionando los eventos ocurridos durante el mes inmediatamente anterior. El formato del reporte se muestra en la ilustración 2 “Formato de reporte desempeño de Disponibilidad".

Ilustración 2 Formato de reporte Desempeño de Disponibilidad

					Codigo:		
					Versión: 01		
PROYECTO							
ZONA					Contacto		
OPERADOR					Cargo		
Fecha Inicio			Fecha Final		Total Minutos		
Ubicación	Dispositivo	BW(MBPS)	Reporte de falla (Ticket)	Medida de Tiempos de Disponibilidad			
				Tiempo de indisponibilidad (Minutos)	Fecha (dd/mm/aaaa)	Total indisponiblidad (Minutos)	Total disponibilidad (%)
DESCRIPCIÓN DE FALLAS Y ACCIONES EJECUTADAS							

Fuente: ANS Comunicaciones

Brevemente se describirán los componentes del reporte en la tabla “Descripción Reporte de Disponibilidad Clientes ANS COMUNICACIONES”.

Componente	Descripción
Proyecto	Nombre del cliente el cual es obtenido del contrato de servicios firmado
Zona	Ubicación de cobertura de ANS COMUNICACIONES
Operador	Encargado de servicio al cliente que genera reporte
Contacto	Persona registrada en la base de datos de la plataforma como responsable de parte del cliente de soporte
Cargo	Cargo de la persona del cliente responsable para el soporte
Fecha de inicio	Día inicial del reporte
Fecha final	Día de resolución del incidente
Total minutos	Suma de los minutos de indisponibilidad de los servicios del cliente
Ubicación	Suma de los minutos de indisponibilidad de los servicios del cliente
Dispositivo	Tipo de enlace afectado por el incidente
BW (Mbps)	Ancho de banda contratado para el servicio afectado
Reporte de falla (ticket):	Número de ticket asociado al incidente reportado
Medida de tiempo de disponibilidad	Esta información está dividida en varios campos: ✓ Tiempo de indisponibilidad (Minutos): Tiempo acordado de indisponibilidad con el cliente. Si hay varios incidentes, se registran los tiempos de cada incidente por separado. ✓ Fecha (dd/mm/aaaa): Fecha del incidente. Si hay varios incidentes, se registran las fechas de cada incidente por separado. ✓ Total Indisponibilidad (Minutos): Sumatoria de los tiempos de indisponibilidad reportados por cada ubicación en el mes del reporte. ✓ Total disponibilidad (%): Porcentaje de disponibilidad total del enlace en el mes del reporte.
Descripción de fallas y acciones ejecutadas	Se realiza un resumen de los eventos reportados y las actividades realizadas para solucionarlos. Se pueden incluir planes de mejora

Tabla 3 Descripción Reporte de Disponibilidad Clientes ANS COMUNICACIONES

El esquema de atención mencionado anteriormente se describe en la ilustración “Esquema de atención”

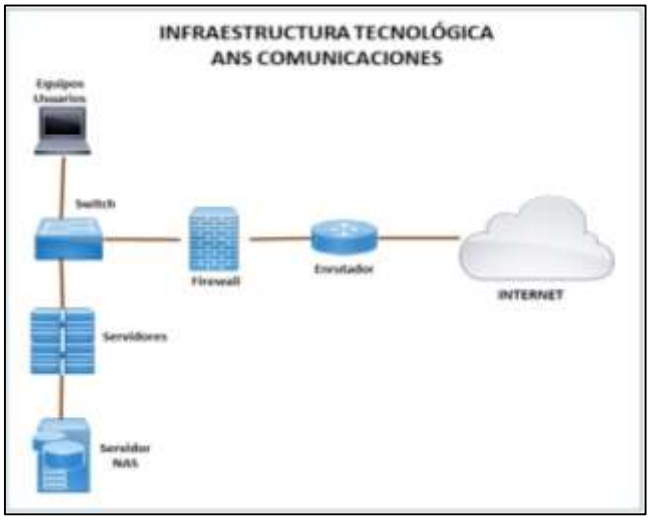
Ilustración 3 Esquema de atención

Fuente: ANS Comunicaciones

2.1.2 Infraestructura Tecnológica y de Sistemas ANS COMUNICACIONES.

Para la operación de este y otros procesos, ANS COMUNICACIONES cuenta con infraestructura propia ubicada dentro de sus instalaciones de Bucaramanga. La arquitectura de esta infraestructura se presenta en la ilustración “Infraestructura tecnológica ANS COMUNICACIONES” y el detalle de la misma se relacionará a continuación:

Ilustración 4 Infraestructura tecnológica ANS COMUNICACIONES



Fuente: El Autor

2.1.2.1 Centro de datos.

Ubicado en las instalaciones de ANS COMUNICACIONES en Bucaramanga. Cuenta con algunas facilidades de estándar de nivel de centro de datos del Uptime institute, sin que se encuentre certificado. Dentro de las facilidades tenemos:

- ✓ Potencia eléctrica: El centro de datos cuenta con respaldo de energía con bancos de baterías alimentados por paneles solares además de la fuente de alimentación de energía pública suministrada por la Electrificadora de Santander. Los circuitos eléctricos se encuentran regulados y entregan potencia a 120 VAC.
- ✓ Control ambiental: La temperatura y la humedad se encuentran controlados por aires acondicionados con capacidad de enfriamiento de 18 mil BTU/hora.
- ✓ Enrutamiento de cables de tensión: Se cuenta con bandejas superiores para enrutar los cableados de alimentación eléctrica.

- ✓ Protección contra incendios: El centro de datos cuenta con detectores de humo para aviso de temperaturas elevadas dentro del Datacenter, el cual activa el sistema de aspersión de gas con agente limpio.
- ✓ Seguridad: El acceso físico se encuentra restringido a personal autorizado. El control se hace a través de tarjeta para abrir las puertas de acceso al Datacenter.

2.1.2.2 Equipos de red.

Para la conexión de los equipos de cómputo de los usuarios de ANS COMUNICACIONES tanto a nivel LAN como de las redes de gestión de los diferentes servicios, se cuenta con los siguientes componentes:

- ✓ Equipos de enrutamiento: Infraestructura de enrutamiento Ubiquiti para la conexión de la red de gestión.
- ✓ Equipos de seguridad perimetral: Infraestructura de seguridad Checkpoint para la habilitación de conexiones seguras a través de internet y habilitar configuraciones de seguridad para la navegación de usuarios.
- ✓ Equipos de switching: Infraestructura Ubiquiti para la conexión de nivel LAN para los dispositivos de usuarios en la sede de ANS COMUNICACIONES en Bucaramanga.

2.1.2.3 Infraestructura de computo.

Para el despliegue de las aplicaciones que usa dentro de sus procesos de negocios, ANS COMUNICACIONES cuenta con servidores DELL con las características descritas en la tabla “Infraestructura ANS COMUNICACIONES”

Componente	Capacidad o Característica
Procesador	Dos Intel® Xeon®con 4 núcleos por procesador
Sistema Operativo	Enterprise Linux SUSE® sobre Linux Enterprise Server VMware® ESXi
Memoria	128 GB DIMM DDR4
Disco Duro	600 Gbytes
Servidor NAS	QNAP 4 Bahias – Dual Core con capacidad de 5 Terabytes de almacenamiento

Tabla 4 Infraestructura ANS COMUNICACIONES

2.1.2.4 Aplicación para gestión de incidentes

Para el proceso de gestión de incidentes, ANS COMUNICACIONES cuenta con la aplicación OSTicket en la cual se registran los incidentes y se realiza la gestión de Asignación, coordinador y base dentro del proceso. Adicionalmente la herramienta genera el informe de desempeño de disponibilidad.

OSTicket es una aplicación desarrollada para dar soportar los requerimientos de empresas que necesitan gestionar incidentes. La plataforma cuenta con varias ediciones para su implementación:

- ✓ Fuente abierta: Es gratuita y solo permite integración con correo electrónico.
- ✓ Nube: Aplicación en servidores de OSTicket. El cliente se conecta a plataforma vía internet y obtiene los servicios estándar de la plataforma (Soporte por correo y telefónico, sesión gratuita, actualizaciones, infraestructura sólida, copias de seguridad diarias).
- ✓ Dispositivo empresarial: Aplicación para montaje en servidores del cliente. Adicional a los servicios de la edición en nube, la aplicación permite desarrollos personalizados para

adaptarse a las necesidades del negocio.

Las características que usa ANS COMUNICACIONES de la aplicación OSTicket se encuentran relacionas en la tabla “Características OSTicket en ANS COMUNICACIONES”.

Características OSTicket	Descripción
Campos Personalizados	Se crearon listas personalizadas de datos para agregar a cada ticket ayudas específicas para que los clientes elijan al crear un ticket.
Columnas y colas personalizadas	Se crearon vistas personales de tickets para especificar qué información de la ciudad donde se presenta el incidente, para asignar el ticket al grupo que maneja dicha ciudad
Filtros de entradas	Si el ticket fue generado por la plataforma WEB, el cliente al parametrizar los campos de ciudad y tipo de enlace, enruta el ticket al grupo de la región y al personal que maneja la tecnología que usa el enlace reportado.
Agente para evitar colisiones	Se usa esta funcionalidad para evitar que se creen respuestas del mismo ticket de manera simultánea
Respuesta automática	Las respuestas automáticas se usan para notificar al cliente la apertura y cierre de los tickets. Se usa como base la información de la base de datos de clientes
Acción de hilo	Se usa esta funcionalidad para realizar notificaciones internas a los grupos de gestión internos o para notificar eventos que no corresponden a la gestión de incidentes. Estos mensajes no llegan a los clientes
Acuerdos de Nivel de Servicio	Se tiene configurado los acuerdos de nivel de servicio para recibir alertas al estar cerca de incumplir con los tiempos de dichos acuerdos
Portal del Cliente	Se habilitó a los clientes este portal para abrir los tickets de requerimientos

Tabla 5 Características OSTicket en ANS COMUNICACIONES

La aplicación es configurada y soportada por personal interno de ANS COMUNICACIONES. El personal usa el soporte que se tiene adquirido con OSTicket en caso de que se presenten problemas con los desarrollos que se hacen dentro de la plataforma o con problemas de segundo o tercer nivel que desborde al personal de desarrollo.

La descripción de los perfiles de usuarios asignados dentro de la plataforma OSTicket se encuentran relacionados en la tabla "Perfiles de usuario OSTicket en ANS COMUNICACIONES".

Perfil de usuario	Características
Administrador de la plataforma	Administración de la base de datos usuarios interna de clientes y agentes de gestión de incidentes.
Supervisores de gestión de incidentes	Seguimiento de los incidentes que se reportan por parte de los clientes.
Gestores de incidentes	Son los usuarios encargados de gestionar con los clientes los incidentes. Hay dos niveles de gestores: ✓ Gestor de primer nivel. ✓ Gestor de segundo nivel.

Tabla 6 Perfiles de usuario OSTicket en ANS COMUNICACIONES

A continuación, se detallarán algunas características de los perfiles mencionados:

- ✓ Administrador de la plataforma: Tiene como tareas la administración de la base de datos usuarios interna de clientes y agentes de gestión de incidentes. Da soporte a incidentes de la aplicación y administra los cambios sobre los campos de datos de la aplicación.
- ✓ Supervisores de gestión de incidentes: Son usuarios de la plataforma. Tienen como labor el seguimiento de los incidentes que se reportan por parte de los clientes. Aunque pueden llegar a realizar las labores de los agentes de gestión de incidentes, no lo realizan salvo en casos de emergencia. Dentro de sus tareas pueden realizar asignación de tickets a gestores de incidentes, reapertura de tickets por solicitud del cliente, asignación de gestores de incidentes a grupos. También están encargados de enviar los reportes de incidentes tanto a los clientes como las áreas de facturación, para realizar la gestión de descuentos sobre los

pagos por incumplimiento de los Acuerdos de Nivel de Servicio.

- ✓ Gestores de incidentes: Son los usuarios encargados de gestionar con los clientes los incidentes. Hay dos niveles de gestores:
  - Gestor de primer nivel: Es personal que realiza interacción con el cliente de manera directa y cuenta con un nivel básico de conocimientos de las tecnologías de servicios ofrecidas por ANS COMUNICACIONES.
  - Gestor de segundo nivel: Es personal que realiza soporte de segundo nivel sobre las plataformas de servicios de ANS COMUNICACIONES. Dan soporte a los gestores de primer nivel.

Dentro de la plataforma OSTicket, tanto los gestores de primer como de segundo nivel tienen las siguientes funciones:

- ✓ Apertura y cierre de tickets.
- ✓ Documentación de las actividades realizadas dentro de los incidentes.
- ✓ Escalamiento a un nivel superior de los incidentes cuando así se requiera.

2.2 Marco teórico

Para desarrollar una auditoría de información dentro del proceso de gestión de incidentes de clientes de ANS COMUNICACIONES S.A., es necesario utilizar y manejar algunos conceptos relacionados a la seguridad informática y de la información, para cualquier entidad del sector público y /o privado.

2.2.1 Sistema de gestión de seguridad de la información.

La seguridad de la información es el conjunto de políticas que las compañías deben adoptar para proteger uno de sus principales activos, la información. El sistema debe velar para que sus procesos estén acorde a los objetivos de negocio y que se basen en las necesidades propias de la compañía. La seguridad de la información debe orientarse a que las medidas aplicadas, tanto preventivas como correctivas, protejan y salvaguarden la confidencialidad, integridad y disponibilidad de los activos de información de la compañía, haciendo especial énfasis en los que sean parte de los procesos sensibles de la compañía.

A continuación resaltaremos algunos conceptos que se desarrollarán dentro de la auditoría:

- ✓ **Seguridad:** Conjunto de sistemas, procesos y medios que buscan reducir, eliminar o controlar riesgos que puedan afectar a los activos de una compañía.
- ✓ **Información:** Es un conjunto organizado de datos que juntos forman un mensaje. Se caracteriza por tener una estructura común.
- ✓ **Confidencialidad:** Principio que busca garantizar que la información será accedida solo por personal que sea autorizado para tal fin.
- ✓ **Integridad:** Este principio busca el aseguramiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ **Disponibilidad:** Algo fundamental dentro de los sistemas de información es que la información sea accesible tanto por los procesos como por los usuarios al momento de ser requerida. Esto es lo que busca este principio.

2.2.2 Auditoría informática.

La auditoría se define como la acción de verificar un determinado hecho o circunstancia de acuerdo a lo planeado. Existen varios tipos de auditoría, las cuales se basan en el entorno en el cual se realizan o el objetivo de la misma.

Las primeras labores de auditoría nacen de la búsqueda de la verdad o falsedad de hechos en juicios basándose en observaciones. Posteriormente, se formaliza la labor de auditoría orientada en verificar procesos contables, generándose varios estándares para realizar esta labor de manera organizada y basada en normas vigentes.

En cuanto a las tecnologías de la información, sobre la década de los 70 en el siglo pasado, el intercambio de experiencias en diferentes campos de las organizaciones permitió generar las primeras normas y procesos de auditoría orientada a procesos de tecnologías de información.

La auditoría de la información se define como los procesos para la verificación de Sistemas de información basada en la recolección, agrupación y evaluación de evidencias, con el fin de salvaguardar los activos de la empresa que mantienen los datos de la organización.

Hay varias normas y estándares para realizar auditorías sistemas de información. Cada una de ellas, aunque tiene sus propios lineamientos, busca gestionar los riesgos de la seguridad de la información con base en las amenazas, vulnerabilidades entre otros principios que relacionaré a continuación:

- ✓ **Riesgo:** La norma ISO 31000:2018 lo define como el efecto de la incertidumbre sobre los objetivos. Puede ser positivo, negativo o ambos y puede abordar, crear o resultar en oportunidades y amenazas. El estándar COBIT 5 amplía su concepto a las tecnologías de información y lo define como (IBARRA & RICO, 2013) *"el riesgo de negocio asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa".*
- ✓ **Amenaza:** Cualquier cosa capaz de actuar contra un activo de manera que pueda causarle daño.
- ✓ **Vulnerabilidad:** Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.
- ✓ **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
- ✓ **Activo:** Según la norma ISO/IEC 133351:2004, un activo es cualquier cosa que tenga valor para la organización. Dentro de un contexto tecnológico, los activos de TI son los recursos tecnológicos con los que toda empresa cuenta para apoyar sus estrategias y sus objetivos de negocio.
- ✓ **Fuente de riesgo:** Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.
- ✓ **Control:** Es cualquier acción que reduce el riesgo mediante la eliminación de las vulnerabilidades o el bloqueo de los agentes de amenaza.
    - o Los controles incluyen procesos, políticas, dispositivos, prácticas u otras acciones que modifican al riesgo.
    - o Los controles no siempre pueden ejercer el efecto modificador previsto o asumido.
- ✓ **Incidente:** acceso, intento de acceso, uso, divulgación, modificación o destrucción no

autorizada de información.

- ✓ **Hallazgo de auditoría:** Se definen como asuntos que llaman la atención del auditor y que deben comunicarse, ya que representan deficiencias importantes que podrían afectar en forma negativa, la capacidad de la organización.
- ✓ **No conformidad:** Según la norma ISO 9000:2005 es un incumplimiento de un requisito del sistema, sea este especificado o no.

2.2.3 Estándar ISO 27002:2013.

Dentro de los estándares y normas existentes a nivel mundial para la estandarización de la seguridad de la información, las normas ISO y sus marcos de referencia son ampliamente reconocidos por su contenido además de provenir de una organización que desde su nacimiento ha evolucionado para buscar las mejoras que permitan a las empresas mejorar su sistemas de información protegidos contra las amenazas crecientes que enfrentan las tecnologías de la información.

Una de las normas ISO que ayuda a las organizaciones a verificar el estado de su Sistema General de Seguridad de la información y a dar las directrices necesarias a implementar para mejorarlo es la norma ISO 27002:2013. Esta norma proporciona recomendaciones de las mejoras prácticas en la gestión de la seguridad de la información, para los diferentes estamentos de la organización y así, implementar o mantener los sistemas de gestión de seguridad de la información.

El estándar asume una visión global de los riesgos de la seguridad de la información para la incorporación de un conjunto amplio de controles de seguridad de la información que sean

coherentes dentro de la organización.

La identificación de los controles con los que debería contar el sistema requiere una planificación cuidadosa y tener el apoyo de todos los empleados de la organización, así como de los accionistas, proveedor u otras partes externas.

La norma ISO 27002:2013 establece tres fuentes principales de requisitos de seguridad:

- ✓ Valoración de los riesgos: Se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la posibilidad de que ocurran, y se estima el impacto potencial.
- ✓ Los requisitos legales, estatutarios, de reglamentación y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios deben cumplir, y su entorno socio-cultural.
- ✓ El conjunto de principios, objetivos y requisitos del negocio para el manejo, procesamiento, almacenamiento, comunicación y archivo de información, que una organización ha desarrollado para apoyar sus operaciones.

La guía brinda orientación sobre gestión de riesgos de seguridad de la información e incluye asesoría sobre valoración, tratamiento, aceptación, comunicación, seguimiento y revisión de riesgos.

La guía establece los siguientes controles de seguridad para ser seleccionados por la organización, teniendo en cuenta que se pueden diseñar nuevos controles para necesidades específicas:

- ✓ Políticas
- ✓ Organización
- ✓ Recursos Humanos
- ✓ Activos
- ✓ Accesos
- ✓ Cifrado
- ✓ Física y ambiental
- ✓ Operativas
- ✓ Telecomunicaciones
- ✓ Adquisición, desarrollo y mantenimiento
- ✓ Suministradores
- ✓ Incidentes
- ✓ Continuidad del negocio
- ✓ Cumplimiento

La guía explica en detalle cada uno de los controles, junto con su guía de implementación. A su vez, la guía incluye información acerca de la selección de controles y otras opciones de tratamiento de riesgos.

La guía ISO 27002 se considera como un punto de partida para el desarrollo de directrices específicas de la organización, teniendo en cuenta que no todos los controles mencionados anteriormente son aplicables.

Una vez desarrolladas las directrices dentro de la compañía, se debe tener en cuenta que la información tiene un ciclo de vida desde su creación y origen, pasando por su almacenamiento, procesamiento, uso y transmisión, hasta se eliminación final. El valor de los activos y los riesgos asociados a estos pueden variar durante su ciclo de vida, pero la seguridad de la información es y será importante en todas las etapas, en mayor o menor medida. Los nuevos desarrollos de sistemas y los cambios en los existentes exigen actualizaciones y mejores en los controles de seguridad, teniendo en cuenta los incidentes reales y los riesgos de seguridad presentes y estimados.

2.2.4 Estándar ISO 31000.

Una de los marcos de referencia más utilizados y de mayor divulgación para la gestión de los riesgos es la norma ISO 31000. Esta norma es aplicable a toda empresa independiente de su tamaño y busca orientar la gestión del riesgo de manera eficaz y eficiente.

La norma refuerza el liderazgo de la Alta dirección en el sistema de gestión del riesgo, desde el gobierno de la empresa hasta los niveles de gestión a través de la creación de valor y utilizando el sistema de gestión como herramienta de seguimiento y control además de servir de apoyo en la toma de decisiones. Esto lo logra a través del alineamiento de la gestión del riesgo con los objetivos de la compañía, su estrategia y no menos importante, la cultura.

La norma contiene varios principios los cuales se encuentran descritos en la tabla “Principios ISO 31000”. Estos principios giran en torno a la creación y protección de valor de la compañía.

Principio	Descripción
Integrada	Gestión del riesgo es parte integral de todas las actividades. Debe estar presente en los procesos de negocio y servir para la toma de decisiones.
Estructurada y Exhaustiva	La gestión del riesgo contribuye a resultados coherentes y comparables. Debe estar definido y contar con su propia estructura.
Personalizada	La gestión del riesgo se adapta y es proporcional a los contextos de las organizaciones. Cada organización define su propio marco.
Inclusiva	Las partes interesadas participan apropiada y oportunamente para que sus puntos de vista sean tenidos en cuenta, a través de una cuidadosa planificación.
Dinámica	Los riesgos son cambiantes, por lo que la gestión del riesgo anticipa, detecta, reconoce y responde a dichos cambios. El marco debe vigilarse y controlarse.
Mejor información disponible	La gestión del riesgo debe basarse en información histórica fiable y tener en cuenta las expectativas a futuro. Se debe comprender lo sensible de las decisiones y que las mismas sean informadas.
Factores humanos y culturales	La gestión del riesgo es influenciada por el comportamiento humano, por ello hay que contar con las opiniones de los interesados.
Mejora continua	El aprendizaje y la experiencia permiten la mejora continua de la gestión del riesgo. La mejor solución es la más simple.

Tabla 7 Principios ISO 31000

La norma establece su proceso para la gestión del riesgo, el cual implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

Los propósitos de los procesos de la norma son descritos en la tabla “Propósitos de procesos de gestión de riesgos – ISO 31000”.

Proceso	Propósito
Comunicación y consulta	Asistir a las partes interesadas a comprender el riesgo, como tomar decisiones y las razones de las acciones específicas necesarias
Alcance, contexto y criterios	Adaptar el proceso de gestión de riesgos para permitir una evacuación del riesgo eficaz y de manera apropiada
Evaluación del riesgo	Identificar, analizar y valorar los riesgos a los que está o estará expuesta la compañía
Tratamiento de riesgos	Seleccionar e implementar las opciones para abordar el riesgo
Grabación e Informes	Documentar e informar el proceso de gestión del riesgo a través de mecanismos apropiados
Monitoreo y revisión	Asegurar y mejorar la calidad y la eficacia del diseño, la implementación y resultados del proceso

Tabla 8 Propósitos de procesos de gestión de riesgos – ISO 31000

2.2.5 Conceptos básicos sobre la gestión de incidencias

De acuerdo a la biblioteca de Infraestructura de Tecnologías de Información (ITIL en inglés) la gestión de incidencias (Jimenez, 2019) es un conjunto de actividades que garantiza que todos los problemas de IT (llamados "incidentes" por ITIL, marco de referencias de las mejores prácticas de ITSM) se registren y progresen de manera eficaz y coherente hasta la resolución.

Los siguientes conceptos hacen parte de la gestión de incidentes, basado en lo establecido por el estándar ITIL:

- ✓ **Acuerdo de Nivel de Servicio (ANS):** o SLA (Service Level Agreement) por sus siglas en inglés, es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.
- ✓ **Escala de tiempos:** A partir de los acuerdos de Niveles de Servicios se establecen los tiempos máximos en los que se deben responder y resolver las incidencias. Se deben usar

herramientas de gestión para el cálculo y la asignación de estas escalas de tiempo, así como para utilizar alertas y escalados para facilitar la respuesta y resolución de las incidencias dentro del tiempo máximo definido.

- ✓ **Modelo de incidencia:** Son los pasos que seguir para la resolución de la incidencia así como el orden cronológico de estos pasos y sus dependencias. El modelo contiene responsabilidades, plazos para la realización de las actividades y procedimientos de escalamiento.

Dentro de los procesos de la gestión de incidentes, identificamos las siguientes actividades que se deben realizar, alineados en el marco de ITIL:

- ✓ **Identificación de incidente:** Se debe asignar un número único para cada incidente el cual recoja datos de ubicación y/o localización. Se recomienda establecer una tipología y codificación de incidencias para facilitar su análisis cualitativo y cuantitativo posterior así como generación de indicadores clave.
- ✓ **Registro de incidente:** Se deja constancia de la incidencia en un registro para que quede documentado y disponible para ser tratado de acuerdo con el procedimiento normalizado.
- ✓ **Categorización de incidente:** La categorización debe ser realmente simple, a fin de que los usuarios de la mesa de ayuda registren sus incidentes de la manera más fácil que sea posible. Se puede agregar más complejidad a los niveles de categorización, pero mantener el nivel inicial simple hará que sea más fácil para los usuarios y los analistas de la mesa de ayuda registrar incidentes con la categoría correcta y asignarlos al equipo de resolución adecuado.

- ✓ **Priorización de incidente:** La priorización es la parte del proceso que ayuda al equipo de resolución a manejar su carga de trabajo. Al establecer las prioridades de los incidentes, la mejor práctica recomienda que se tenga en cuenta:
    - Impacto: el grado en que la prestación de servicios se interrumpió dentro de la organización y el efecto que esta interrupción tiene en otras áreas de la infraestructura.
    - Urgencia: la velocidad con que el incidente debe ser resuelto.
- ✓ **Diagnosticar:** Esta es la parte donde se decide si el incidente puede ser solucionado o necesita ser escalado a otros miembros de soporte o a un equipo en particular. En un entorno de mesa de ayuda, el primer analista evalúa si se puede corregir de inmediato el incidente que se está reportando o si es necesario escalarlo al soporte de segundo nivel. Los scripts, las bases de datos de errores conocidos (KEDBs) y las bases de conocimientos, pueden ayudar a mejorar la tasa de resolución en la primera respuesta, otros procesos ayudarán con esto.
- ✓ **Remitirlo a un nivel superior de soporte:** Si un incidente no puede ser resuelto en el primer punto de contacto (en una llamada o cuando el usuario carga el ticket) entonces es necesario que sea escalado en pos de restaurar el servicio. Existen dos tipos de escalamiento en una mesa de ayuda típicamente configurada:
    - Funcional
    - Jerárquico
- ✓ **Investigación y Diagnóstico:** La investigación y el diagnóstico ocurren durante cada etapa del ciclo de vida del incidente junto con la monitorización, las actualizaciones y la comunicación. Tan pronto como se registra el incidente, el usuario de la mesa de ayuda comienza a evaluar la

llamada (o el ticket que cargó el usuario final) y a recopilar información. Esto puede tener como resultado, una solución de primera respuesta, o el incidente puede escalarse al soporte de segundo nivel, y más allá, donde la investigación y el diagnóstico continuarán hasta que el problema haya sido resuelto y el servicio normal haya sido restaurado.

- ✓ **Resolución y restablecimiento del servicio:** Una vez todo está solucionado se deben realizar pruebas y volver a probar en busca un enfoque de mejora continua.
- ✓ **Cierre del incidente:** Se debe actualizar el registro de incidentes con lo que pasó y lo que se hizo para solucionarlo antes de cerrarlo.

2.2.6 Normas internacionales de auditoría.

Las Normas Internacionales de Auditoría son un conjunto de estándares internacionales de obligatorio cumplimiento para auditores que realizan auditorías de estados financieros. Establece los objetivos globales del auditor independiente y explica el alcance de la auditoría para cumplir con los objetivos establecidos en la misma. Las Normas son conocidas como NIA y son emitidas por el Consejo de normas Internacionales de auditoría y seguimiento y aseguramiento IAASSB-IFAC, por sus siglas en ingles.

Las NIA establecen entre otros:

- ✓ Objetivos globales del auditor: Las NIA definen entre otras que la información obtenida de la auditoría está libre de incorrección material por fraude o error, la emisión de un informe sobre el estado de lo auditado y salvedades en caso de que no pueda obtenerse información con seguridad razonable.
- ✓ Definiciones: Las NIA definen dentro de ellas términos como los marcos de información

aplicables, marco de imagen fiel, evidencia de auditoría, riesgo de auditoría, auditor, riesgo de detección, estados financieros, entre otros para que el auditor tenga claridad sobre los mismos.

- ✓ Requerimientos: Dentro de las NIA se definen los requerimientos de ética relativa a la auditoría, el escepticismo profesional, el juicio profesional, la evidencia de auditoría suficiente y adecuada y riesgo de auditoría.

Estas definiciones se encuentran dentro de la NIA 200, la cual profundiza cada una de estas definiciones. En la tabla "Contenido de las NIAs" se encuentra un resumen de las mismas.

NIA	Contenido
NIA 200	Objetivos generales del auditor independiente y la conducción de una auditoría de acuerdo con NIA
NIA 210	Acuerdo en las condiciones de los compromisos de auditoría
NIA 230	Documentos de auditoría
NIA 240	Responsabilidades del auditor en materia de fraude en una auditoría
NIA 250	Consideraciones de las leyes y reglamentos en una auditoría
NIA 260	Comunicación con la Gerencia y responsabilidades de la dirección

Tabla 9 Contenido de las NIAs

2.3 Marco jurídico

ANS COMUNICACIONES se encuentra regida por varias leyes y normas dadas su naturaleza y campos de acción.

2.3.1 Leyes de la república.

2.3.1.1 Ley 142 de 1994.

(Congreso, Ley 142, 1994) Esta ley se aplica a los servicios públicos domiciliarios de acueducto, alcantarillado, aseo, energía eléctrica, distribución de gas combustible, telefonía fija pública básica

conmutada y telefonía local móvil en el sector rural. Dentro de los artículos de esta ley, el número 51 obliga a las empresas de servicios públicos a contratar auditorías externas de gestión y resultados. El articulo número 53 indica que la superintendencia de Servicios públicos debe establecer los sistemas de información que deben organizar y mantener actualizados las empresas de servicios públicos.

2.3.1.2 Ley 143 de 1994.

(Congreso, Ley 143, 1994)Ley por la cual se establece el régimen para la generación, interconexión, transmisión, distribución y comercialización de electricidad en el territorio nacional, se conceden unas autorizaciones y se dictan otras disposiciones en materia energética. Esta ley establece las condiciones para las empresas que generan energía, independiente de su origen y la forma de integrarse al sistema interconectado nacional.

2.3.1.3 Ley 1341 de 2009.

(Congreso, Ley 1341, 1994)Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones – TIC -, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Esta ley define el uso y manejo que se debe dar al espectro electromagnético y crea a la Agencia Nacional del Espectro como ente encargado de supervisa el uso y gestión de este recurso.

2.3.2 Resoluciones y decretos del ministerio de las tecnologías de la información y las comunicaciones.

2.3.2.1 Resolución 202 de 2010.

(MINTIC, Resolución 202, 2010)Del Ministerio de tecnologías de la información y las comunicaciones por la cual se expide el glosario de definiciones conforme a lo ordenado por el inciso 2º del artículo 6º de la ley 1341 de 2009.

Esta resolución define la terminología a adoptar dentro de la ley mencionada, con base en los postulados de la Unión Internacional de las Telecomunicaciones (UIT). La resolución contiene definiciones para términos como Interconexión, interoperatividad, proveedor de aplicaciones, proveedor de contenido, proveedor de redes y servicios de telecomunicaciones, red de telecomunicaciones, servicios de telecomunicaciones, telecomunicación y usuario.

2.3.2.2 Decreto 2044 de 2013.

(MINTIC, Decreto 2044, 2013)Del Ministerio de tecnologías de la información y las comunicaciones por el cual se reglamenta los artículos 12 y 68 de la ley 1341 de 2009. Decreto que tiene como objeto establecer los requisitos y las condiciones para la renovación de los permisos de uso del espectro radioeléctrico.

2.3.2.3 Decreto 542 de 2014.

(MINTIC, Decreto 542, 2014) Del Ministerio de tecnologías de la información y las comunicaciones de Por el cual se reglamentan los artículos 10, 13 y 36 de la ley 1341 de 2009 y se dictan otras disposiciones Decreto que tiene por objeto definir la contraprestación periódica por la provisión de redes y servicios de telecomunicaciones, así como la base sobre la cual se aplica dicha contraprestación.

2.3.2.4 Resolución 917 de 2015.

(MINTIC, Resolución 917, 2015)Del Ministerio de tecnologías de la información y las comunicaciones por la cual se determinan las garantías para cubrir riesgos en materia de telecomunicaciones y de servicios postales que define las garantías que deben pagar las empresas del sector de las telecomunicaciones por cumplimiento en el pago de contraprestaciones y eventuales sanciones de las que puedan ser objetos.

2.3.2.5 Decreto 1078 de 2015.

(MINTIC, Decreto1078, 2015)Del Ministerio de tecnologías de la información y las comunicaciones por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones que contiene los aspectos a tener en cuenta dentro del sector de las tecnologías de la información y las comunicaciones.

2.3.2.6 Resolución 1260 de 2016.

(MINTIC, Resolución 1260, 2016)Por la cual se dictan disposiciones en relación con la autoliquidación y pago electrónico de las contraprestaciones que se den pagar a favor del fondo de Tecnologías de la Información y las comunicaciones así como los intereses derivados de las mismas y las sanciones.

Resolución que tiene como objeto el procedimiento para la autoliquidación y pago electrónico de las contraprestaciones que se deban pagar al fondo de Tecnologías de la Información y las comunicaciones derivadas de la provisión de redes y servicios de telecomunicaciones, el uso del espectro radioeléctrico o la prestación de servicios postales.

2.3.3 Resoluciones de la Comisión de Regulación de Comunicaciones.

2.3.3.1 Resolución 3066 de 2011.

(Comisión de Regulación de Comunicaciones, Resolución 3066, 2011)Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones.

Resolución que establece el régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones. Establece las directrices para la interacción de los usuarios y proveedores en aspectos claves como la seguridad de la red y de los servicios contratados.

2.3.3.2 Resolución 3789 de 2012.

(Comisión de Regulación de Comunicaciones, Resolución 3789, 2012)Por la cual se desarrolla el literal f) del parágrafo 10 del artículo 11 de la Ley 1369 de 2009, en lo relacionado con la imposición de sanciones, se modifica el artículo 6 de la Resolución CRC 3151 de 2011 Y se dictan otras disposiciones.

Esta resolución define los procedimientos para las contribuciones con destino a la Comisión de Regulación de la Comunicaciones, así como los procedimientos por sanciones, multas e incumplimientos en el pago de las mismas.

2.3.3.3 Resolución 3067 de 2011.

(Comisión de Regulación de Comunicaciones, Resolución 3067, 2011)Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones.

Resolución que establece las obligaciones generales, obligaciones de calidad para el servicio de acceso a internet, comunicaciones de voz y para mensajes de texto.

2.3.3.4 Resolución 5050 de 2016.

(Comisión de Regulación Comunicaciones, 2016)Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones

Esta resolución contiene la compilación de las normas de carácter general expedidas por la CRC.

2.3.3.5 Resolución 4838 de 2015.

(Comisión de Regulación de Comunicaciones, Resolución 4838, 2015)Por la cual se regulan los aspectos relacionados con la obligación de separación contable por parte de los Proveedores de Redes y Servicios de Telecomunicaciones y Operadores de televisión por suscripción y se dictan otras disposiciones.

Resolución que establece los lineamientos contables para la prestación de los servicios de telecomunicaciones y su registro en los sistemas de contabilidad de las compañías prestadoras de servicios de telecomunicaciones.

2.4 Marco geográfico

De acuerdo a (ANS Comunicaciones, www.anscomunicaciones.com.co, 2018) ANS COMUNICACIONES es una compañía del sector de las telecomunicaciones que presta sus servicios a nivel nacional. Es un grupo empresarial que desarrolla y suministra soluciones innovadoras de servicios de comunicaciones, energía y sistemas inteligentes que acercan la tecnología a los hogares, comunidad y empresas para generar bienestar y desarrollo sostenible.

2.4.1 Misión ANS COMUNICACIONES.

De acuerdo a (ANS Comunicaciones, 2018) la misión de ANS es “Proporcionamos bienestar y

desarrollo sostenible a la sociedad con la generación de soluciones innovadoras, especializadas y flexibles para el suministro de servicios de telecomunicaciones con la más alta calidad y amplía cobertura, que nos permite anticiparnos a las necesidades de comunicación y conectividad de nuestros clientes."

2.4.2 Visión ANS COMUNICACIONES.

De acuerdo a (ANS Comunicaciones, 2018) para el 2028 ANS Comunicaciones consolidará su liderazgo nacional y extenderá su participación en Latinoamérica a través de la gestión integral de infraestructura de telecomunicaciones para operadores y clientes corporativos y, el suministro de conectividad en zonas de baja cobertura; reconocidos por su excelencia en el servicio y su alta capacidad de generar soluciones innovadoras adaptadas a las necesidades de sus clientes con criterios de desarrollo sostenible.

2.4.3 Portafolio de servicios.

ANS Comunicaciones cuenta con un amplio portafolio de servicios de infraestructura eléctrica y de telecomunicaciones, los cuales brinda a nivel nacional.

La tabla "Servicios de ANS Comunicaciones" nos brinda un resumen del portafolio mencionado y algunas de sus características.

Servicio	Características
Ultimas millas	✓ Redes Wifi ✓ Redes Punto a Punto y Redes Punto – Multipunto ✓ Enlaces Tipo Carrier.
Unidades móviles	Unidades que cuentan con 12, 18 y 24 metros de altura sobre tráiler de doble troque para ubicación de antenas.
Energía	Soluciones de suministro eléctrico con paneles solares.
Redes cableadas	✓ Soluciones de cableado estructurado. ✓ Soluciones de cableado en fibra óptica.
Networking	Suministro, instalación y soporte de telefonía IP.
Infraestructura	✓ Coubicación de nodos ✓ Soluciones eléctricas para telecomunicaciones. ✓ Seguridad – videovigilancia.
Soluciones especializadas	✓ Gestión y Monitoreo de Redes ✓ Diseño de Redes

Tabla 10 Servicios de ANS Comunicaciones

2.4.4 Cobertura.

ANS COMUNICACIONES brinda servicios en varias regiones del país, teniendo presencia en las regiones que se pueden apreciar en la ilustración “Cobertura ANS Comunicaciones.

Ilustración 5 Cobertura ANS Comunicaciones

Fuente: ANS Comunicaciones

Adicionalmente, ANS COMUNICACIONES está ampliando sus servicios a Perú, específicamente en la ciudad de Pucallpa, en la provincia de Coronel Portillo.

2.5 Estado del arte

2.5.1 Certificaciones ANS COMUNICACIONES

ANS COMUNICACIONES ha adelantado procesos para su Sistema de Gestión Integral (S.G.I ANS COMUNICACIONES). Las certificaciones obtenidas a la fecha de la presentación de este documento se encuentran en la tabla "Certificaciones ANS COMUNICACIONES".

Certificación	Alcance
ISO 9001 SC-CER358401	Certificación del Sistema de Gestión de Calidad ANS COMUNICACIONES.
ISO 14001 SA-CER358400	Certificación del Sistema de Gestión Ambiental.
OHSAS 18001 OS073-1	Certificación de control de riesgos de seguridad y salud ocupacional.
Norsok S-006 NK-402-1	Certificación de gestión ambiental, de seguridad industrial y de salud Ocupacional.

Tabla 11 Certificaciones ANS COMUNICACIONES

Estas certificaciones y los procesos adelantados para obtener las mismas se enfocaron en aspectos relacionados con la gestión integral, ambiental, salud ocupacional y riesgos de seguridad general, pero ninguna se ha relacionado con el objetivo de este estudio.

2.5.2 Estudios relacionados con procesos de gestión.

En revisiones hechas sobre estudios con un enfoque similar al de la auditoría que se está planteando en este proyecto, encontramos los siguientes que nos brindan luces de cómo se abordaron los aspectos involucrados en el presente proyecto.

2.5.2.1 Estudio de guía de gestión de riesgos.

El primer estudio que revisamos, es el planteado por un grupo de estudiantes de la Universidad Católica de Colombia como trabajo de grado que se tituló (Arias Reyes, Diaz Rodriguez, & Vargas Carvajal, 2014) *"ELABORACIÓN DE UNA GUÍA DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA NTC-ISO 31000 PARA EL PROCESO DE GESTIÓN DE INCIDENTES Y PETICIONES DE SERVICIO DEL ÁREA DE MESA DE AYUDA DE EMPRESAS DE SERVICIOS DE SOPORTE DE TECNOLOGÍA EN COLOMBIA*". En este trabajo, se planteó como objetivo general la elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000, para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda. Se planteó cuatro frases para su desarrollo, relacionados en la tabla "Fases desarrollo trabajo de grado Universidad Católica de Colombia año 2014*"*.

Fase	Planteamiento para desarrollo
Fase 1	Validar una empresa real de tecnología en Colombia
Fase 2	Análisis de los procesos, subprocesos y actividades obtenidas para generar una matriz de riesgos
Fase 3	Realizar la revisión de la norma ISO 31000 con la cual se comenzará a realizar la guía y se complementará con la norma NTC 5254
Fase 4	Realizar la implementación de la norma ISO 31000

Tabla 12 Fases desarrollo trabajo de grado Universidad Católica de Colombia año 2014

Revisando lo evaluado en este trabajo, se ha encontrado que su enfoque se dio sobre las mesas de

ayuda de servicios de tecnología y que si bien evaluó el proceso y los sub procesos de la atención de mesa de ayuda, algo similar a lo que abarca este proyecto, el enfoque se dio sobre la gestión de riesgos del proceso y no en el Sistema General de la Seguridad de la Información. Luego de la aplicación de la norma ISO 31000, las conclusiones de este trabajo apuntaron a dar recomendaciones de mejoras en los procesos que involucran servicios de IT pero no abarcan al Sistema General de Seguridad de la Información.

2.5.2.2 Estudio de guía de Sistema de gestión de seguridad de la información.

Adicionalmente, revisamos un estudio planteado sobre las normas de la serie ISO 27000. El estudio se tituló (Picón Carrascal, 2016) "ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013", desarrollado como trabajo final del Master Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones de la Universidad Oberta de Catalunya en asociación con la Universitat Autónoma de Barcelona, la Universitat Rovira Virgili y la Universitat de les Illes Balears. El trabajo fue desarrollado en Colombia y tuvo como objetivo general el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información para brindar apoyo para proteger los activos de información del ICFES. Este trabajo se basa en la norma ISO 27001:2013, buscando la identificación de los procesos del ICFES y los riesgos de su Sistema de Gestión de la Seguridad de la Información. El enfoque de este trabajo se da sobre la madurez de los controles establecidos en la norma ISO 27001:2013 en el ICFES y da un diagnóstico de su estado actual en la compañía a través de la emisión de los conceptos de auditoría. Esta auditoría se centró en la evaluación del Sistema Gestión de la Seguridad de la Información ya existente en el ICFES, pero sus resultados fueron netamente cuantitativos y no

dieron recomendaciones para la implementación de mejoras con base en la norma mencionada.

3 MARCO METODOLÓGICO

3.1 Tipo de investigación

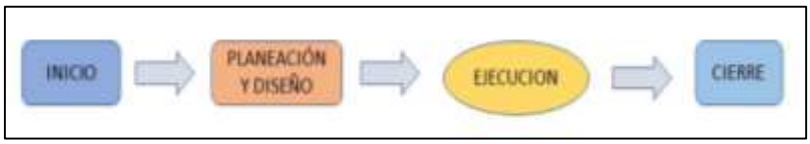
Estrategia de investigación bajo el paradigma positivista con enfoque de investigación cuantitativa, un alcance descriptivo y un diseño experimental transversal.

3.2 Diseño de la investigación

3.2.1 Proceso de investigación.

Las fases del proyecto que se elaborará se presentan en la ilustración "Fases del proyecto de investigación" y se basan en la metodología Tradicional de gestión de proyectos (TMP por sus siglas en ingles).

Ilustración 6 Fases del proyecto de investigación



Fuente: El Autor

3.2.1.1 Inicio.

En la fase de inicio, se realizarán las labores de levantamiento de información necesario para el

desarrollo del proyecto. Esta labor se realizará con base en el conocimiento que se tiene de la empresa y tendrá como herramientas principales entrevistas que nos darán el contexto del negocio de ANS COMUNICACIONES. Se hará énfasis en determinar los procesos internos y externos que son pertinentes a su visión y misión y que podrían llegar a afectar la capacidad para el alcance de sus logros y poner en riesgo al sistema de seguridad de la información. Dentro del contexto se identificarán las partes interesadas dentro del proceso de gestión de incidentes de clientes de Networking de ANS COMUNICACIONES.

La etapa de inicio entregará al proyecto el contexto de la empresa el cual incluirá los contextos tanto interno como externo y los factores de riesgos con su descripción.

3.2.1.2 Planeación y diseño.

Con base en el contexto realizado en la etapa inicial, se procederá con la evaluación del sistema de control interno del proceso de gestión de incidentes de clientes de Networking de ANS COMUNICACIONES. Esta evaluación se realizará de la siguiente manera:

3.2.1.2.1 Identificación de riesgos.

Una vez contextualizado el proceso de gestión de incidentes de Networking, se procederá a evaluar los riesgos de seguridad de la información. Esto a partir de la identificación de los activos, amenazas y las vulnerabilidades a las que se encuentran expuestos dichos activos. La identificación usará como base las matrices de Riesgos de la norma ISO 31000.

3.2.1.2.2 Identificación de controles.

Una vez definidos los riesgos, se procederá a analizar los controles que se podrían implementar por parte de ANS COMUNICACIONES para mitigar el impacto en los activos y el negocio. La definición de controles estará basada en la norma NTC-ISO/IEC 27002 y se usará como herramientas las matrices de riesgos y controles de dicha norma.

3.2.1.2.3 Diseño de pruebas de auditoría.

Una vez definidos los controles aplicables al proceso objeto de la auditoría, se procederá con el diseño de las diferentes pruebas a realizarse a los componentes del Sistema de Información del proceso. Estas pruebas estarán enfocadas en auditar el estado de la Disponibilidad, Integridad y Continuidad de la información del proceso evaluado. Las pruebas se diseñarán con base en los formatos de auditoría propuestos por las normas ISO e ISACA y su estructura estará enfocada en evaluar de la mejor manera los controles propuestos a los riesgos identificados.

La etapa de planeación y diseño entregará al proyecto matrices de riesgos y control, así como los formatos de pruebas de auditoría para su ejecución.

3.2.2.2 Ejecución.

En la etapa de ejecución se procederá a realizar las tareas plasmadas en las pruebas de auditoría, teniendo como base los formatos y procedimientos allí diseñados. La ejecución de las pruebas se

realizará con la ayuda del personal dueño y responsables del proceso de gestión de incidentes.

Cada una de las pruebas de auditoría se deberá documentar y almacenar dentro del legajo permanente de auditoría que se tendrá disponible para el proyecto. El personal de auditoría documentará el resultado obtenido durante la prueba (hallazgos y no conformidades) en el formato de la prueba.

De cada una de las pruebas, se analizará los hallazgos encontrados que servirán como base para determinar las recomendaciones a dar para la mejora del proceso.

La etapa de ejecución entregará al proyecto los hallazgos de la auditoría.

3.2.1.4 Cierre.

En la etapa de cierre, se elaborará el informe de auditoría con las recomendaciones, directrices y acciones a implementar al Sistema General de Seguridad de la Información del proceso de gestión de incidentes de clientes de Networking de ANS COMUNICACIONES.

3.2.2 Diseño de instrumentos.

Para la ejecución de las etapas anteriormente mencionadas, utilizaremos los siguientes instrumentos diseñados para obtener la mayor cantidad de información posible por parte de los involucrados en el proceso que auditaremos así como para ilustrar de la mejor manera la auditoría propuesta en el proyecto.

3.2.2.1 Entrevistas.

Usaremos las entrevistas como instrumento para obtener la información específica sobre el Sistema de Información del proceso de gestión de Incidentes de Clientes de ANS COMUNICACIONES y el estado de su seguridad informática. Se realizarán tres entrevistas a diferentes miembros del grupo de operaciones de ANS COMUNICACIONES, las cuales mantendrán el mismo formato.

3.2.2.1.1 Entrevista a gerencia de operaciones.

Características de la entrevista	
Fecha de aplicación	29/05/2019
Tipo de entrevista	Entrevista a profundidad
Enfoque	Sujeto – Objeto
Objetivos	✓ Identificar los procesos involucrados en la gestión de incidentes de clientes de ANS COMUNICACIONES. ✓ Conocer las expectativas de la gerencia con relación al sistema de gestión de la seguridad de la información.
Quien realiza entrevista	Jose Miguel Fuentes Caro
Nombre Entrevistado	Adriana Rodriguez
Edad	40 años
Ocupación	Ingeniera Industrial
Nivel de educación	Profesional
Relación con el proyecto	Gerente de operaciones ANS COMUNICACIONES

Tabla 13 Características de la entrevista a gerencia de operaciones

Cuestionario Preparado
A. Introducción
La entrevista está enfocada en obtener la información desde el punto de vista de la gerencia de ANS COMUNICACIONES, para ver el enfoque que desde la gerencia se tiene tanto del proceso como del Sistema de gestión de la Seguridad de la información.
B. Identificar Entrevistados y participantes
Adriana Rodriguez es la encargada de la gerencia de operaciones de ANS COMUNICACIONES y es parte de la junta directiva de la compañía. Adriana lleva en el cargo cerca de 15 años y tiene a su cargo el proceso de gestión de incidentes de networking.
C. Preguntas de expectativas de sistemas de gestión de la seguridad de la información.
C.1 Indíquenos la cantidad de empleados de ANS COMUNICACIONES. C.2 ¿Qué tipo de estructura organizacional tiene ANS COMUNICACIONES? C.3 ¿Las políticas corporativas son definidas por un área específica? C.4 ¿Cómo se controla el cumplimiento de las políticas corporativas? C.5 ¿Las políticas corporativas son comunicadas a los empleados de la organización? ¿De qué manera? C.6 ¿Cómo se tramitan los requerimientos entre las áreas de la organización? C.7 ¿Existe una política de adquisiciones para los activos de la organización? C.8 ¿Se cuentan con manuales de operaciones? ¿Dónde se almacenan? C.9 ¿La infraestructura de la empresa (Servidores, equipos de computo, equipos de redes) es propia? C.10 ¿Cuenta la empresa con políticas para el control de activos? C.11 ¿Cuentan con políticas de continuidad de negocio? C.12 ¿La empresa cuenta con políticas de acceso a la información? C.13 ¿Cuenta la compañía con medios de respaldo para la infraestructura (UPS, Planta eléctrica? C.14 ¿Existen políticas para el envío de la información a clientes y proveedores? C.15 ¿Cuenta la compañía con políticas de acceso de redes Wifi? C.16 ¿Las políticas de seguridad están alineadas con los objetivos de la empresa? ¿De qué manera? C.17 ¿Cuenta el personal con los perfiles requeridos para su cargo? C.18 ¿Cómo se realiza el diseño para la implementación de las aplicaciones en la compañía? C.19 ¿Los procesos de entrega de aplicaciones en producción están acompañados de capacitaciones para los usuarios? C.20 ¿La empresa tiene contemplados operaciones a través de internet?
D. Preguntas procesos gestión de incidentes de clientes de ANS COMUNICACIONES.
D.1 ¿Qué tipo de políticas tiene definidas el área de operaciones? D.2 ¿Con relación a la seguridad, que políticas tiene la organización dispuestas? D.3 ¿Existen políticas de contratación de personal de gestión de incidentes? D.4 ¿El área de operaciones tiene un presupuesto independiente? D.5 ¿Cuántas personas realizan la gestión de incidentes de networking? D.6 ¿Cómo se manejan los escalamientos dentro del área de operaciones? D.7 ¿Dichos procesos cumplen las políticas establecidas dentro del área de operaciones?
E. Cierre de la entrevista

3.2.2.1.2 Entrevista a supervisor de operaciones.

Características de la entrevista	
Fecha de aplicación	29/05/2019
Tipo de entrevista	Entrevista a profundidad
Enfoque	Sujeto – Objeto
Objetivos	✓ Identificar los recursos involucrados en el proceso de gestión de incidentes de clientes de ANS COMUNICACIONES. ✓ Conocer cómo es la estructura del Sistema de Seguridad de la información de ANS COMUNICACIONES. ✓ Identificar cómo se realiza el control de los lineamientos y políticas definidos dentro del proceso de gestión de incidentes.
Quien realiza entrevista	Jose Miguel Fuentes Caro
Nombre Entrevistado	Carlos Ballen
Edad	25 años
Ocupación	Ingeniero de sistemas
Nivel de educación	Profesional
Relación con el proyecto	Supervisor mesa de operaciones ANS COMUNICACIONES

Tabla 14 Características entrevista supervisor de operaciones

Cuestionario Preparado
A. Introducción
La entrevista está enfocada en obtener la información que el supervisor del proceso de gestión de incidentes maneja y como desde las labores operativas es percibida y manejada a seguridad de la información.
B. Identificar Entrevistados y participantes
Carlos lleva en el cargo cerca de 2 años y tiene a su cargo la supervisión del personal de gestión de incidentes y a su vez es responsable de generar reportes de gestión tanto de los incidentes como de la operación del personal.
C. Preguntas identificación recursos involucrados.
C1. ¿El acceso al cuarto de equipos donde se encuentran los servidores de las aplicaciones se encuentra restringido? ¿Cómo se definen los procedimientos de acceso al Datacenter? C2. ¿Se cuenta con medios de respaldo para la información de incidentes? C3. ¿Los accesos a las aplicaciones cuentan perfiles? C4. ¿Cuenta la empresa como una política de manejo de respaldos de información (Discos duros, cintas)? C5. ¿Qué tipo de contingencias se tiene contempladas y ante qué clase de eventos?

D. Preguntas de conocimiento de estructura del Sistema de gestión de la seguridad de la información
D1. ¿Qué políticas están definidas dentro del proceso de gestión de incidentes? D2. ¿Conoce como las políticas se orientan a los objetivos del negocio de la empresa? D3. ¿Los roles de las personas que atienden la gestión de incidentes incluyen las funciones definidas a cada rol? D4. Cuando el personal se encuentra fuera de la oficina ¿Puede conectarse a las plataformas de gestión de incidentes? D5. ¿Cómo es el proceso de alta y baja de usuarios en las aplicaciones de gestión de incidentes? D6. ¿Quién realiza el control de acceso a los equipos de red y seguridad? D7. ¿Se encuentran las redes de usuarios de gestión de incidentes separadas de las redes de los demás departamentos funcionales? D8. ¿Los accesos a las aplicaciones cuentan perfiles? D9. ¿Sabe si en los contratos laborales existen cláusulas contractuales para el manejo de información confidencial? D10. ¿Quién es el encargado de asignar los accesos a las aplicaciones? D11. ¿Los usuarios se pueden conectar a las aplicaciones de gestión de incidentes a través de la red Wifi? D12. ¿Cuentan las aplicaciones de gestión de incidentes con controles de acceso?
E. Preguntas identificación control de los lineamientos y políticas dentro del proceso de gestión de incidentes
E1. ¿El personal de gestión de incidentes conoce las políticas de seguridad de la empresa? ¿Cómo son notificados de las mismas? E2. ¿Los perfiles de las personas que atienden la gestión de incidentes son validados previo a su ingreso? ¿usted los valida? E3. ¿Realiza seguimiento al cumplimiento de las políticas establecidas por la empresa? ¿De qué manera lo hace? E4. ¿Cuentan los dispositivos de red y seguridad con controles de acceso? E5. ¿Pueden los usuarios compartir información de los perfiles asignados? E6. ¿Qué tipos de controles se tienen para el acceso al Datacenter? E7. ¿Hay definidos protocolos para la información que es enviada vía correo electrónico? E8. ¿Hay alguna aplicación que tenga usuario con una misma clave?
F. Cierre de la entrevista

3.2.2.1.3 Entrevista a operador de gestión de incidentes de clientes de networking.

Características de la entrevista	
Fecha de aplicación	29/05/2019
Tipo de entrevista	Entrevista a profundidad
Enfoque	Sujeto – Objeto
Objetivos	✓ Conocer cómo interactúan los usuarios de las aplicaciones.
Quien realiza entrevista	Jose Miguel Fuentes Caro
Nombre Entrevistado	Alejandro Marín
Edad	22 años
Ocupación	Técnico de sistemas
Nivel de educación	Técnico
Relación con el proyecto	Operador de gestión de incidentes ANS COMUNICACIONES

Tabla 15 Características entrevista operador de gestión de incidentes de clientes Networking

Cuestionario Preparado
A. Introducción
La entrevista está enfocada en obtener la información desde el punto de vista operativo de ANS COMUNICACIONES, para ver el enfoque de los usuarios de las plataformas de gestión de incidentes y su interacción con los clientes.
B. Identificar Entrevistados y participantes
Alejandro lleva en el cargo cerca de 1 año y tiene a su cargo la atención de clientes de networking.
C. Preguntas contextualización de usuarios de aplicaciones.
C1. ¿Ha sido informado de las políticas de la empresa con relación a la seguridad? C2. ¿Sobre qué tipo de activos se enfoca la seguridad de la empresa? C3. ¿Se le informó al momento de ingresar a la compañía del rol y las responsabilidades asignadas a su cargo? ¿de qué manera? C4. ¿Se conecta a las aplicaciones de la empresa a través de internet? C5. ¿Proporcionó la información de su experiencia y formación al momento del ingreso a la compañía? C6. ¿Conoce las maneras de reportar incidentes de seguridad en la compañía? C7. ¿Conoce las políticas de manejo de activos de la compañía? C8. ¿Guarda de maneta segura el equipo de computo asignado por parte de la compañía? C9. ¿Firmó algún acta de entrega al momento de recibir los activos? ¿La tiene guardada? C10. ¿Usa dispositivos de almacenamiento externos para transferir información de la compañía?

C11. ¿Tiene un usuario propio para el acceso a las aplicaciones corporativas? C12. ¿Su contraseña de acceso cumple con alguna política de asignación de claves? C13. ¿Conoce la política de manejo de claves? C14. ¿Puede usted acceder a información sensible de otras áreas? C15. ¿Comparte o ha compartido usted la información de usuario y clave de acceso a las aplicaciones? ¿Por qué lo ha hecho? C16. ¿Usa la misma clave para acceder a las diferentes plataformas? C17. ¿Conoce las políticas de acceso al Datacenter de la compañía? C18. ¿Conoce los procedimientos de reporte para novedades que se detecten en la seguridad de los accesos a las áreas restringidas?
D. Cierre de la entrevista

3.2.2.2 Diseño de formatos de auditoría.

Para el desarrollo de la auditoría propuesta a la Seguridad del Sistema de Información del proceso de gestión de incidentes de clientes de ANS COMUNICACIONES, se propone los siguientes formatos para la ejecución de las diferentes etapas de la auditoría.

3.2.2.2.1 Matriz de riesgos.

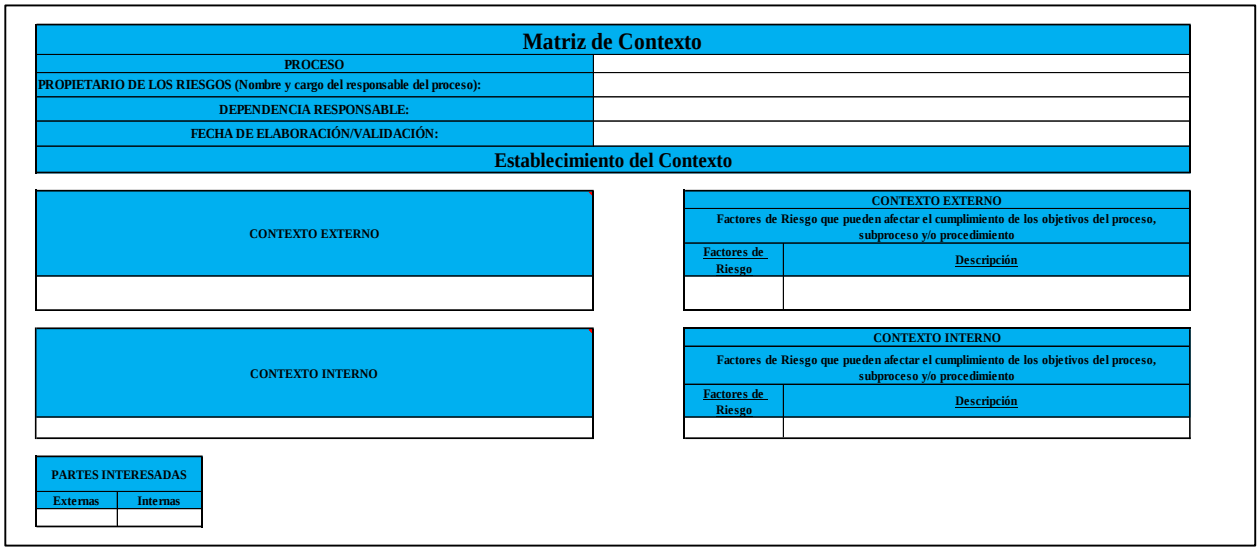
La matriz de riesgos nos permite realizar una valoración de los riesgos a los cuales está expuesto el proceso a auditar, basada en análisis de la información entregada por la compañía a auditar y enfocada en el proceso sujeto de la auditoría.

La matriz se compone de los siguientes campos:

- ✓ Contexto ANS: Este campo nos muestra el proceso a auditar, los responsables del proceso, dependencias involucradas, fechas de realización del formato y la información pertinente al contexto en el cual se desarrolla el proceso a auditar. Se incluye información de contexto tanto interna como externa y los factores de riesgos identificados por parte del auditor. La ilustración “Formato Contexto ANS”

nos muestra el formato planteado.

Ilustración 7 Formato de contexto ANS



Matriz de Contexto	
PROCESO	
PROPIETARIO DE LOS RIESGOS (Nombre y cargo del responsable del proceso):	
DEPENDENCIA RESPONSABLE:	
FECHA DE ELABORACIÓN/VALIDACIÓN:	

Establecimiento del Contexto

CONTEXTO EXTERNO

CONTEXTO EXTERNO	
Factores de Riesgo que pueden afectar el cumplimiento de los objetivos del proceso, subproceso y/o procedimiento	
Factores de Riesgo	Descripción

CONTEXTO INTERNO

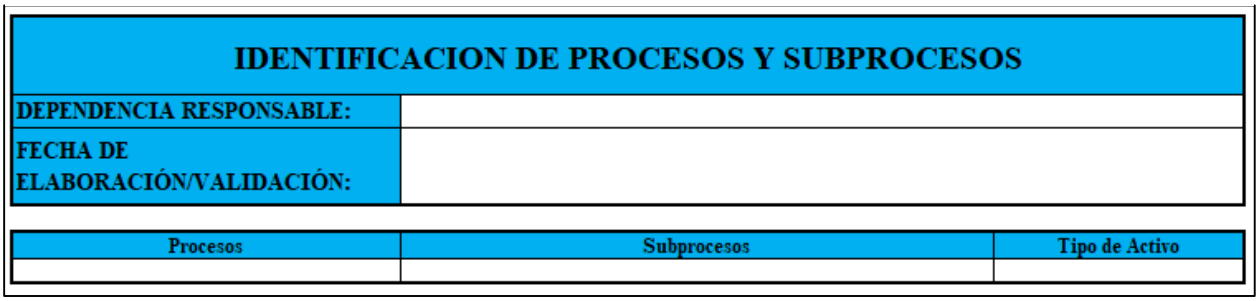
CONTEXTO INTERNO	
Factores de Riesgo que pueden afectar el cumplimiento de los objetivos del proceso, subproceso y/o procedimiento	
Factores de Riesgo	Descripción

PARTES INTERESADAS	
Externas	Internas

Fuente: El Autor

- ✓ Identificación de procesos: Este formato busca mostrar los diferentes subprocesos y activos identificados dentro del proceso macro objetivo de la auditoría. La ilustración "Formato Identificación de procesos" muestra el contenido del mismo.

Ilustración 8 Formato Identificación de procesos



IDENTIFICACION DE PROCESOS Y SUBPROCESOS	
DEPENDENCIA RESPONSABLE:	
FECHA DE ELABORACIÓN/VALIDACIÓN:	

Procesos	Subprocesos	Tipo de Activo

Fuente: El autor

- ✓ Valoración de activos: En este formato se plasma la información de los activos identificados y valorarlos con base en varios aspectos dentro de los que se destaca su impacto en la triada de seguridad (Confidencialidad, Integridad y Disponibilidad), el valor corporativo del activo, el nivel de acceso de los usuarios, si el activo contiene o no información personal y de usuarios, la ubicación del activo, propietario, responsable, custodio y una breve reseña de justificación del análisis hecho. La ilustración "Formato Valoración de Activos" nos muestra los campos anteriormente mencionados y su ubicación dentro del formato.

Ilustración 9 Formato Valoración de Activos

Fuente: El Autor

- ✓ Matriz de riesgo: Una vez relacionados los activos y su valoración, procederemos a obtener el nivel de riesgo al que se encuentra expuesto cada uno de los activos del proceso auditado. Esta evaluación quedará relacionada en la matriz de riesgos, donde de un lado realizamos la identificación del riesgo a través de la relación de amenazas y vulnerabilidades a las que está expuesta cada uno de los activos identificados en la valoración y el riesgo al que están expuestos. Teniendo como base la identificación del riesgo, se realizará el análisis del riesgo que busca

identificar la probabilidad de ocurrencia, su impacto en la triada de seguridad y el impacto total del riesgo sobre el activo, para de esta manera obtener el riesgo inherente al que está expuesto. Esta matriz nos permitirá de un lado entender el nivel de riesgo al que están expuestos los activos pero más relevante aún, orientar los esfuerzos de la auditoría a través del cálculo del riesgo para maximizar los esfuerzos de la auditoría sobre los procesos y activos que se encuentren en un nivel de riesgo inherente alto. La ilustración "Formato matriz de riesgos" muestra los diferentes campos mencionados anteriormente.

Ilustración 10 Formato matriz de riesgos

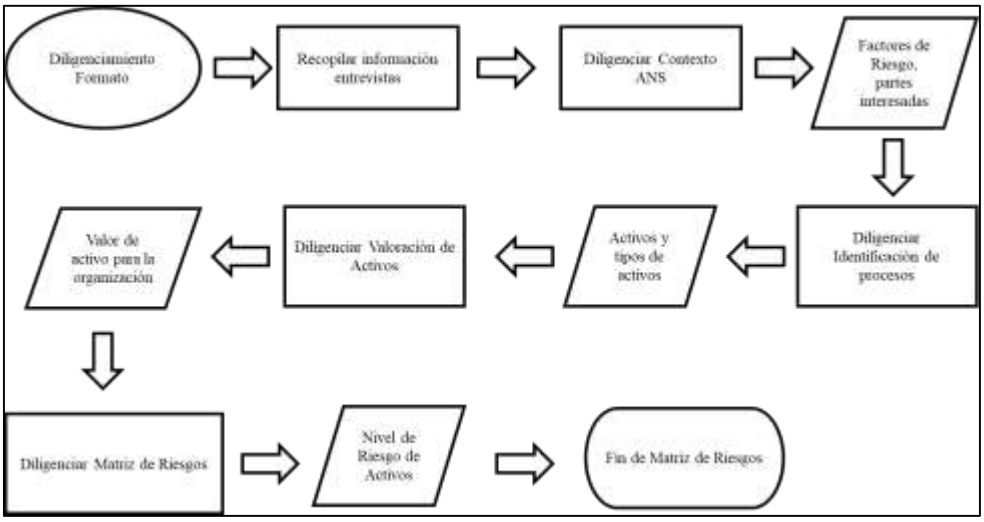
Matriz de Riesgos	
PROCESO:	
PROPIETARIO DE LOS RIESGOS:	
DEPENDENCIA RESPONSABLE:	
FECHA DE ELABORACIÓN/VALIDACIÓN:	

	Identificación del Riesgo								Análisis del Riesgo						
Proceso	Subproceso	Código Riesgo	Nombre del Activo	Descripción Activo	Tipo Activo	Amenaza	Vulnerabilidades	Redacción del Riesgo	Probabilidad de Ocurrencia		Impacto Credibilidad e Imagen	Impacto Información	Impacto Legal	Impacto Financiero	Impacto Total

Fuente: El Autor

Los formatos serán diligenciados de manera secuencial, dado que la información contenida en cada uno de ellos depende de la información que se obtenga del formato inmediatamente anterior, teniendo en cuenta que todos guardan una estrecha relación dado que son parte de la evaluación de un mismo proceso y de los activos involucrados en el. La ilustración "Diagrama de flujo diligenciamiento matriz de Riesgos" nos ayuda a entender la forma en la cual se realizará el diligenciamiento.

Ilustración 11 Diagrama de flujo diligenciamiento matriz de Riesgos



Fuente: El Autor

3.2.2.2.2 Formato matriz de riesgos y controles ANS COMUNICACIONES.

La matriz de riesgos y controles nos permitirá evaluar los riesgos a los que se encuentran expuestos los activos relacionados en la matriz de riesgos y definir los controles que se requieren para mitigar el impacto de los riesgos. La matriz re riesgos y controles tiene como base la matriz de riesgos del numeral 3.2.2.2.1 y tiene los siguientes campos adicionales:

- ✓ Matriz de controles: En la matriz de controles relacionamos los controles que se deberían implementar dentro de la organización para mitigar el impacto que pueden tener las amenazas y vulnerabilidades sobre el Sistema de gestión de la seguridad de la información. En la matriz se relacionarán los controles de los dominios que se han identificado se deben evaluar dentro de la auditoría y como resultado de la evaluación de controles tendremos el ajuste de la probabilidad e impacto que nos

permitirá mostrar a la organización como los controles a implementar o implementados apoyarán al negocio en la mitigación de los riesgos. La ilustración "Matriz de controles" muestra los diferentes campos mencionados anteriormente.

Ilustración 12 Matriz de controles

Matriz de Controles	
PROCESO:	
PROPIETARIO DE LOS RIESGOS:	
DEPENDENCIA RESPONSABLE:	
FECHA DE ELABORACIÓN/VALIDACIÓN:	

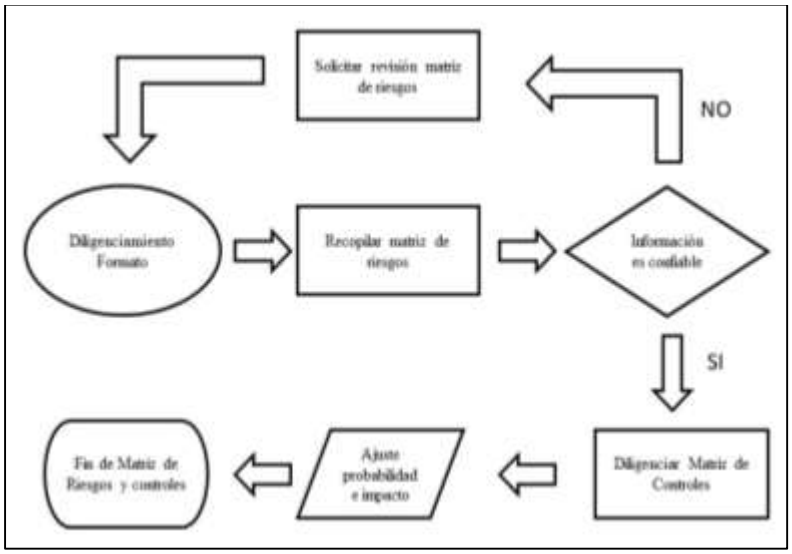
Evaluación de Controles								
Dominio de control ISO 27002	Código de objetivo de control Norma ISO 27002	Código del Control auditoria	Nombre del control	Descripción del control	Tipo	Implementación	Documentación	Percepción de Efectividad

Fuente: El Autor

Los formatos de la matriz serán diligenciados de manera secuencial y tendrá como requisito previo el diligenciamiento de la Matriz de riesgos para entrar en el análisis de los controles. Previo al diligenciamiento del formato de la matriz de controles, se deberá validar que la información fuente proveniente de la matriz de riesgos nos permita definir los dominios que serán parte de la auditoría y que permitirán enfocar los esfuerzos de la organización en mejorar su Sistema de Gestión de la seguridad de la información.

La ilustración "Diagrama de flujo diligenciamiento matriz de Riesgos y controles" nos ayuda a entender la forma en la cual se realizará el diligenciamiento.

Ilustración 13 Diagrama de flujo diligenciamiento matriz de Riesgos y controles



Fuente: El Autor

3.2.2.2.3 Guías de auditoría.

La guía de auditoría contiene la información base para la aplicación de los procesos de auditoría que nos permitirán validar el estado de los diferentes componentes del Sistema de Gestión de la seguridad de la información. En ella se establecen tanto los objetivos como el procedimiento que se realizará y que permitirán al auditor obtener herramientas para el diagnóstico y evaluación del proceso auditado dentro de la norma establecida como parámetro de la auditoría, en este caso la ISO 270002:2013. Cada guía será diseñada para auditar los controles en los dominios definidos en el proyecto y se compondrán del mismo formato base, aunque se debe tener en cuenta que cada guía tendrá sus propios objetivos y procedimientos a aplicar.

El formato contiene los siguientes campos:

- ✓ PRUEBA NUMERO: Campo que relaciona el número consecutivo de la prueba.
- ✓ AREA: Área o departamento dueña del proceso.
- ✓ FECHA: Fecha de elaboración de la guía.
- ✓ OBJETIVOS: Objetivos de la guía de auditoría. Dichos objetivos deben estar alineados a los controles objeto de la guía.
- ✓ TIPO: Se relaciona el tipo de prueba a realizar, presencial, virtual o Mixta.
- ✓ NORMATIVA APLICABLE: Se relaciona la norma base con la que se está adelantado la guía.
- ✓ RECURSOS NECESARIOS PARA APLICARLA: Se enumeran los recursos tanto humanos como de computo necesarios para adelantar la guía.
- ✓ PROCEDIMIENTO A EMPLEAR: Se realiza una descripción detallada de los procedimientos a ejecutar para realizar la auditoría. Se deben incluir cada uno de los procedimientos que se consideren necesarios.
- ✓ Elaborado por: Nombre del auditor que ejecutó la guía.
- ✓ Fecha: Fecha en que se entrega la guía de auditoría.
- ✓ Revisado por: Nombre de personal que realiza revisión de la guía de auditoría.
- ✓ Fecha: Fecha en que se realiza la revisión de la guía.

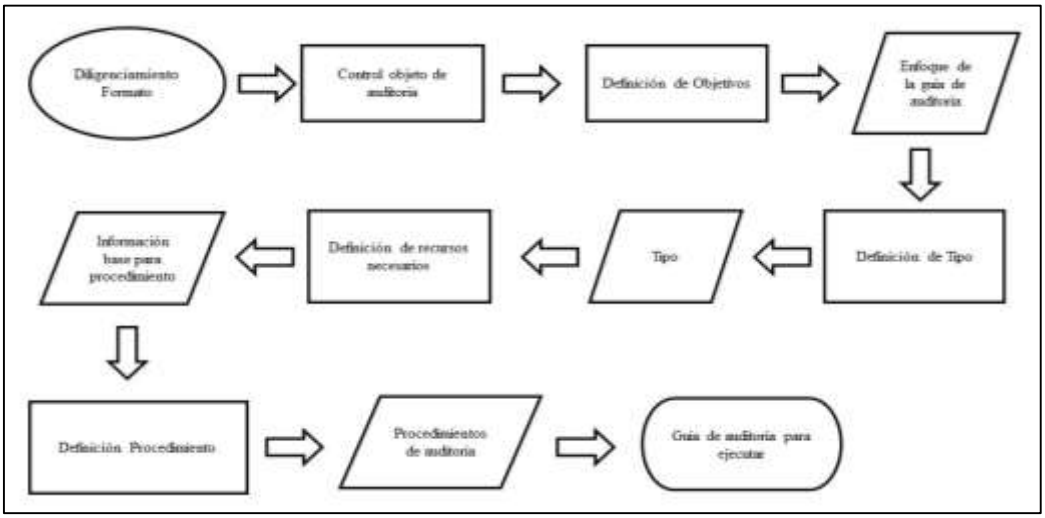
A continuación, se relaciona el formato que se propone para la guía de auditoría:

AUDITORÍA SISTEMAS **PRUEBA NUMERO:**		
PROGRAMA DE AUDITORÍA		
AREA:	**FECHA:**	
PROCESO:		
PROCEDIMIENTO DE AUDITORÍA	**REF. P/T**	**POR**
OBJETIVOS:		
TIPO:		
NORMATIVA APLICABLE:		
RECURSOS NECESARIOS PARA APLICARLA **INFORMACIÓN**		
PROCEDIMIENTO A EMPLEAR		
Elaborado por: _____ Fecha: __/__/____ Revisado por: _____ Fecha: __/__/____		

La ilustración “Diagrama de flujo diligenciamiento guía de auditoría” nos ayuda a entender la

forma en la cual se realizará el diligenciamiento de la guía de auditoría.

Ilustración 14 Diagrama de flujo diligenciamiento guía de auditoría



Fuente: El Autor

3.2.2.2.4 Prueba de auditoría.

El formato de prueba de auditoría permite documentar las pruebas planteadas en la guía de auditoría. La misma hace parte de los papeles de trabajo y su objetivo es, más allá de documentar la prueba, la misma incluye los hallazgos de auditoría y las conclusiones que el auditor considera son relevantes de la prueba realizada. Los campos incluidos dentro del formato prueba de auditoría son los siguientes:

- ✓ Número de Prueba de auditoría: Número de la guía de auditoría a la que corresponde la prueba.
- ✓ Prueba

- Nombre de la prueba: Nombre correspondiente al número de la guía de auditoría de la prueba.
- Objetivo: Objetivo de la prueba de auditoría. Debe corresponder a los objetivos de la guía de auditoría.

✓ Procedimiento

- Fecha: Fecha de la ejecución de la prueba de auditoría.
- Validación: Se relaciona el detalle de las pruebas ejecutadas. Las mismas deben conservar coherencia con la guía y se deben ceñir a las pruebas de auditoría de la guía de auditoría correspondiente a la prueba.
- Elaborado por: Nombre del auditor que realizó las actividades de la guía de auditoría.
- Conclusión: Se debe documentar si desde el punto de vista del auditor la prueba es Satisfactoria o no satisfactoria.

La prueba de auditoría se relaciona a continuación:

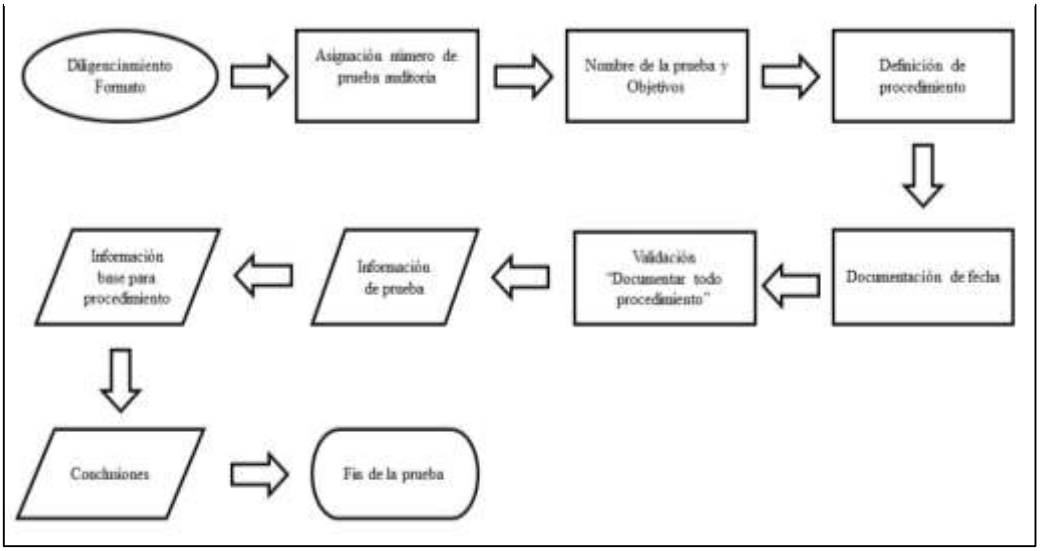
Número de Prueba de auditoría

Prueba	Procedimiento
Nombre de la prueba: **Objetivo:**	**Fecha**: **Validación:** **Elaborado por**: **Conclusión:**

La ilustración “Diagrama de flujo diligenciamiento prueba de auditoría” nos ayuda a entender la

forma en la cual se realizará el diligenciamiento de la prueba de auditoría.

Ilustración 15 Diagrama de flujo diligenciamiento prueba de auditoría



Fuente: El Autor

3.3 Aplicación de la metodología de investigación.

3.3.1 Etapa de inicio.

Con base en lo propuesta en la etapa de diseño, se realizaron entrevistas a personal de ANS Comunicaciones con diferentes grados de responsabilidad dentro del proceso de gestión de incidentes de cliente de Networking. Las entrevistas fueron ejecutadas vía Meet de Google y vía correo y se encuentran disponibles para su visualización en la página https://youtu.be/bVvVHFl8CoA

Se entrevistaron a la gerente de operaciones de ANS COMUNICACIONES, ingeniera Adriana

Rodriguez, al supervisor de operaciones ingeniero Carlos Ballen y al operador de gestión de incidentes Alejandro Marín.

A continuación relacionaremos de manera resumida los resultados de cada una de las entrevistas.

De la entrevista a la gerencia de operaciones, los puntos importantes a resaltar se presentan en la tabla "Resultados entrevista gerencia de operaciones".

Objetivo planteado	Resultados y Conclusiones de la entrevista
Identificación de los procesos involucrados en la gestión de incidentes de clientes de ANS COMUNICACIONES.	✓ La estructura de la compañía es jerárquica, teniendo divisiones por áreas que responden a la gerencia general. ✓ La empresa cuenta con un sistema integrado de gestión, el cual es transversal a todas las operaciones de la empresa. ✓ La compañía cuenta con procedimientos establecidos para varios aspectos que involucran la seguridad tanto física como lógica. ✓ ANS Comunicaciones cuenta con infraestructuras propias pero adquiridas en modalidad de leasing operativo. ✓ La empresa tiene procesos informáticos que ya se encuentran alojados fuera de sus instalaciones, lo que muestra su enfoque en migrar servicios a nubes privadas y públicas.
Conocimiento de las expectativas de la gerencia con relación al sistema de gestión de la seguridad de la información.	✓ La empresa cuenta políticas establecidas para varios frentes como la seguridad industrial y de infraestructura que usan de base para los demás aspectos de seguridad, incluyendo la informática. ✓ Los empleados son informados de las políticas y sus cambios a través de capacitaciones continuas, programadas por las áreas responsables de los cambios. ✓ Las políticas de seguridad de la compañía se enfocan en controlar el acceso de los usuarios a las diferentes plataformas y de las distintas formas que se pueden disponer para tal fin.

Tabla 16 Resultados entrevista gerencia de operaciones

Luego realizamos la entrevista al supervisor de operaciones de ANS Comunicaciones quien tiene a cargo a los operadores de gestión de incidentes. Los puntos importantes a resaltar se presentan en la tabla "Resultados entrevista supervisor de operaciones".

Objetivo planteado	Resultados y Conclusiones de la entrevista
Identificación de los recursos involucrados en el proceso de gestión de incidentes de clientes de ANS COMUNICACIONES.	✓ La infraestructura con la que cuenta ANS Comunicaciones se encuentra alojada en un Datacenter que cuenta con respaldos de energía y de comunicaciones pero que solo cuenta con un medio de control para acceso (tarjeta de acceso). ✓ Se cuentan como medio de respaldo para la información a la nube de google. ✓ Hay contingencias establecidas para eventos de fallas de infraestructura eléctrica y de acceso del personal a las instalaciones de la empresa, pero no se evidencia planes de contingencia de otra clase de eventos.
Conocimiento de la estructura del Sistema de Seguridad de la información de ANS COMUNICACIONES.	✓ Se cuentan con políticas definidas para la gestión de incidentes. Las mismas van orientadas a dar la mejor atención a los clientes, que es uno de los pilares de ANS Comunicaciones. ✓ Los usuarios tienen perfiles de acuerdo a su rol. ✓ Aunque las aplicaciones cuentan con controles de acceso, no hay definidas políticas de asignación de altas y bajas de los mismos. ✓ Existe una política para la divulgación de información de clientes, aunque solo orientada a la información que se envía a clientes en el proceso de gestión de incidentes pero no para otros procesos. ✓ Los usuarios cuentan con la opción de conectarse por la red Wifi a las aplicaciones de la empresa, aunque los usuarios de gestión de incidentes no usan esta opción dado que cuentan con un punto de red asignado en su puesto de trabajo. ✓ Para acceder al Datacenter de la compañía, se cuentan con políticas para el acceso de personal tanto interno como externo. Dicho procedimiento no es conocido por parte de los empleados que no hacen parte del área responsable de dicha infraestructura. ✓ Los usuarios se pueden conectar a la aplicación de gestión de incidentes a través de internet si así lo requieren, aunque continúan usando el mismo usuario y clave sin ningún tipo de medio de autenticación adicional.
Identificación de cómo se realiza el control de los lineamientos y políticas definidos dentro del proceso de gestión de incidentes.	✓ Existe una política corporativa para la divulgación de la información de políticas de seguridad, en cualquiera de sus vertientes. La misma es notificada a los empleados al momento de su ingreso y actualizada por medio de capacitaciones continuas. ✓ Las políticas corporativas son actualizadas a través de capacitaciones, pero no se encuentra un proceso que permita establecer su conocimiento y grado de cumplimiento.

Tabla 17 Resultados entrevista Supervisor de operaciones

Por último, se realiza entrevista a una de las cuatro personas de operaciones de ANS Comunicaciones quien tiene a cargo la gestión de incidentes de clientes. Los puntos importantes a resaltar se presentan en la tabla "Resultados entrevista operador de gestión de incidentes".

Objetivo planteado	Resultados y Conclusiones de la entrevista
Conocer cómo interactúan los usuarios de las aplicaciones.	✓ Los operadores conocen su rol dentro de la gestión de incidentes. ✓ El personal conoce la existencia de las políticas de seguridad integrado de gestión, pero solo tienen conocimiento de que deben reportar cualquier tipo de incidente al coordinador de HSEQ. ✓ Los usuarios de la aplicación de gestión de incidentes cuentan con un usuario asignado de acuerdo a su perfil, pero se encontró que para el personal en entrenamiento se comparten los usuarios y claves de los operadores que ya cuentan con la asignación de usuario. ✓ Los usuarios asignan su clave de acceso de acuerdo a su propio criterio, sin que exista una política de generación de claves seguras. ✓ El personal no tiene como parte de sus políticas de seguridad la no ubicación de información sensible sobre sus escritorios de trabajo. ✓ Se evidencia que la misma tarjeta de acceso al edificio de ANS Comunicaciones es utilizada para el control de acceso a áreas sensibles de la empresa. ✓ No hay una política para el cierre de sesión automático de los equipos de computo del personal de gestión de incidentes. ✓ Dado que se tiene respaldo de la información en la nube de google a través de la aplicación google drive, el personal no usa dispositivos de almacenamiento externos como CD o USB. ✓ Los operadores de gestión de incidentes no acceden a información sensible de otras áreas pero no por conocimiento de una política que lo establezca sino porque no lo han requerido. ✓ Los operadores conocen la política de divulgación de información de incidentes de clientes pero basado en un formato predefinido para notificaciones pero el formato no incluye limitaciones en la información que se puede enviar a los clientes o terceros.

Tabla 18 Resultados entrevista operador de gestión de incidentes

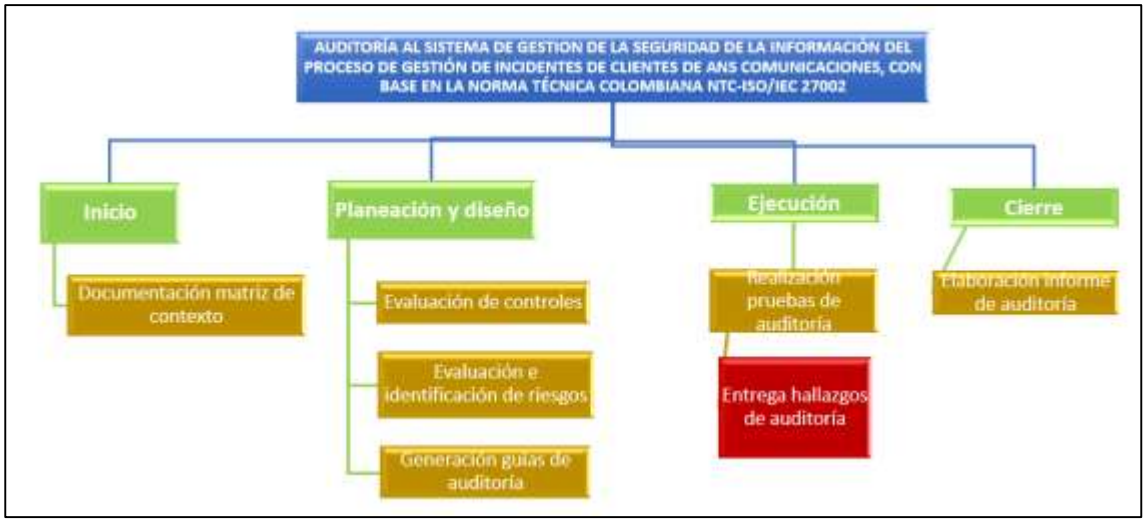
Con base en los resultados de las entrevistas, se procede a documentar la matriz de contexto del formato de matriz de riesgos ANS Comunicaciones.

3.3.2 Etapa de planeación y diseño.

Según La Guía del PMBOK®, (PMBOK, s.f.) *"la Estructura de Desglose del Trabajo (EDT) es una descomposición jerárquica, orientada al producto entregable del trabajo que será ejecutado por el equipo del proyecto, para lograr los objetivos del proyecto y crear los productos entregables requeridos".*

Se presenta un modelo de EDT que acopla la secuencia de actividades a seguidas dentro del desarrollo del proyecto para cumplir con el objetivo principal y que es ilustrado en la ilustración "Estructura de Desglose de Trabajo (EDT).

Ilustración 16 Estructura de Desglose de Trabajo (EDT)



Fuente: El Autor

El cronograma de actividades estimado para la ejecución de la auditoría se muestra en la ilustración "Cronograma de actividades".

Ilustración 17 Cronograma de actividades

No	ACTIVIDADES	SEMANAS								Total actividad	
		MES 1				MES 2					
		1	2	3	4	5	6	7	8	Semanas	% de avance en el tiempo
1	Inicio									1	13%
2	Documentación matriz de contexto									2	25%
3	Evaluación de controles									3	38%
4	Evaluación e identificación de riesgos									4	50%
5	Generación de guías de auditoria									5	63%
6	Realización pruebas de auditoria									6	75%
7	Entrega hallazgos de auditoria									7	88%
8	Elaboración de informe de auditoria									7	88%
9	Cierre /Entrega Final									8	100%
	TOTAL:									8	100%

Fuente: El Autor

A continuación, se describen las actividades relacionadas en el cronograma:

- ✓ Inicio: Se obtendrá a través de entrevistas y del marco geográfico de la empresa la información para la contextualización.
- ✓ Documentación matriz de contexto: Con base en la información del contexto se diligenciará la matriz de contexto para identificar los activos de información de la empresa.
- ✓ Evaluación de controles: Se realizará la evaluación de los controles aplicables a las amenazas y vulnerabilidades de los activos información.
- ✓ Evaluación e identificación de riesgos: Se realizará la evaluación de riesgos obteniendo el cálculo del riesgo inherente definiendo los controles a auditar.

- ✓ Generación de guías de auditoría: Se diseñarán las guías de auditoría para evaluar el estado de los controles definidos con base en el riesgo inherente.
- ✓ Realización de pruebas de auditoría: Se realizarán las pruebas de auditoría con base en las guías generadas.
- ✓ Entrega hallazgos de auditoría: Se realizarán la documentación de los hallazgos encontrados en las pruebas de auditoría.
- ✓ Elaboración de informe de auditoría: Una vez analizadas los hallazgos de auditoría, se procederá a generar el informe de auditoría para ser presentado a la empresa.
- ✓ Cierre/entrega final: Se realizará cierre del proyecto con la información recolectada en cada una de las etapas.

Para la etapa de planeación y diseño, tomamos como base la documentación de los formatos establecidos en el diseño de la investigación.

3.3.2.1 Evaluación e identificación de los riesgos.

Inicialmente se realiza la identificación de los riesgos a los cuales se encuentra expuestos ANS Comunicaciones. Dentro de la matriz que se diligenció en el Anexo A "Formato matriz de riesgos ANS Comunicaciones", identificamos los subprocesos asociados al proceso de gestión de incidentes de Networking, objeto de la auditoría. Cada uno de los subprocesos se asoció al tipo de activo que representa para la empresa. La tabla "Subprocesos y tipos de activos" plasma los resultados de la identificación del proceso de gestión de incidentes de clientes de Networking de ANS Comunicaciones.

Proceso	Subprocesos	Tipo de Activo
Gestión de incidentes de clientes de networking	Telefonía para atención de incidentes	Servicio
	Apertura vía WEB de incidentes	Servicio
	Apertura de ticktes de incidentes	Servicio
	Almacenamiento de información de incidentes	Información
	Plataforma de atención de incidentes	Software
	Generación de reportes de disponibilidad	Software
	Calculo de descuentos por indisponibilidad	Información
	Plataforma de gestión de equipos	Servicio
	Gestión de personal de incidentes	Recurso Humano
	Contratación de personal de incidentes	Recurso Humano
	Capacitación de personal de incidentes	Recurso Humano
	Configuración de acceso a clientes a apertura de incidentes	Información
	Alta y baja de usuarios de herramienta de gestión de incidentes	Información
	Configuración de acceso a la herramienta vía internet	Servicio
	Configuración de acceso a la herramienta vía LAN	Servicio
	Acceso a internet de la herramienta de atención de incidentes	Servicio
	Configuración de equipos de seguridad para la conexión de personal de incidentes vía internet	Hardware
	Aprovisionamiento de servidores para aplicaciones	Hardware

Tabla 19 Subprocesos y tipos de activos

Posteriormente, se procede a realizar la valoración de activos asociados a al proceso de gestión de incidentes. Como resultado de la valoración, podemos resaltar que de los activos analizados, el de mayor valoración tiene para el proceso de gestión de incidentes es la aplicación OSTicket, calificada con un valor muy alto. Posteriormente encontramos ubicados con un valor de calificación alto las aplicaciones de correo y almacenamiento de google, los canales de internet de la empresa, el personal de Soporte de operaciones, la infraestructura de servidores para las aplicaciones y por último el Datacenter de ANS Comunicaciones. Y con una valoración de calificación media encontramos las bases de datos de clientes, proveedores e inventarios, el sistema de gestión de red Ubiquiti, la aplicación de telefonía Asterisk y el personal de soporte de IT.

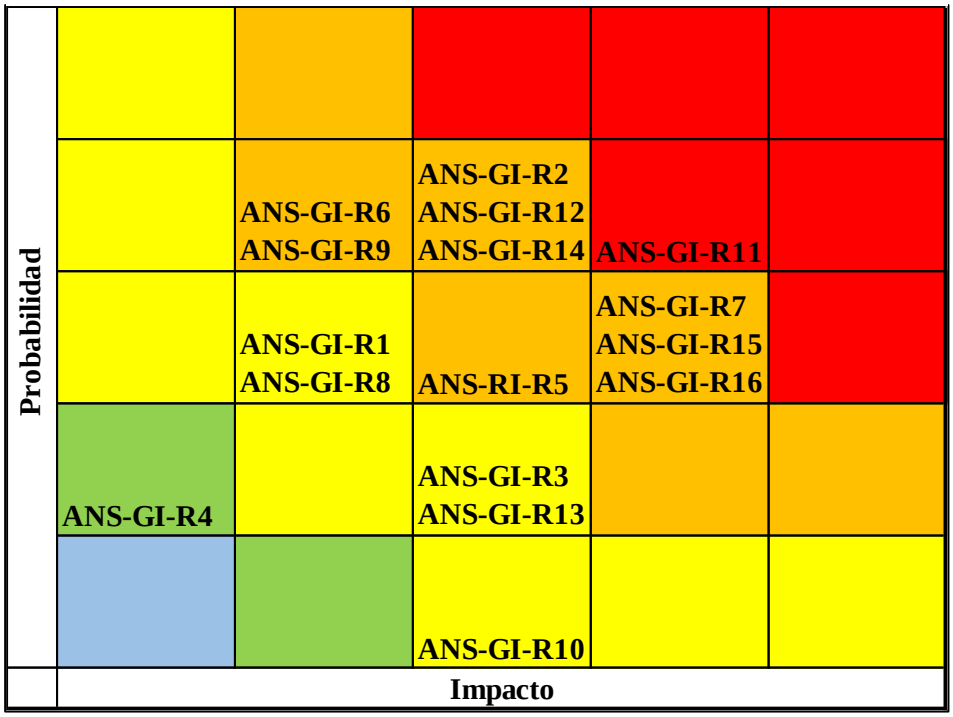
Los resultados completos de la valoración pueden ser consultados en el Anexo A "Formato matriz de riesgos ANS Comunicaciones", hoja Valoración de Activos.

Con la valoración de activos realizada, se inició la elaboración de la matriz de riesgos. Dentro de la matriz de riesgos relacionamos las amenazas y vulnerabilidades así como el riesgo a los que está expuesta la empresa por cada una de las amenazas y vulnerabilidades. Una vez listados los aspectos mencionados en el párrafo anterior, procedemos a realizar el análisis del riesgo, teniendo como base la probabilidad de ocurrencia y el impacto de cada uno de los riesgos.

Los riesgos detectados frente al proceso de gestión de incidentes se encuentran relacionados en el formato del Anexo A, Formato matriz de riesgos ANS Comunicaciones, hoja Matriz de riesgos.

Como resultado, tenemos la gráfica de nivel de riesgo inherente la cual se encuentra en la ilustración "Nivel de riesgo inherente".

Ilustración 18 Nivel de riesgo inherente



Fuente: El Autor

A partir del resultado de cálculo del riesgo inherente, observamos que 7 riesgos tienen un nivel de riesgo inherente elevado lo cual los hace objeto de controles por parte de la auditoría.

El detalle de los riesgos con un alto grado de riesgo inherente se encuentra la tabla “Listado de riesgos con nivel elevado riesgo inherente”.

Código Riesgo	Nombre del Activo	Amenaza	Vulnerabilidades	Riesgo
ANS-GI-R2	Aplicación OSTicket	Pérdida de integridad en la información	Carencia de políticas de control de acceso a las aplicaciones de soporte	Perdida reputacional por modificación no autorizada de la información sensible de incidentes de clientes.
ANS-GI-R7	Infraestructura de servidores para aplicaciones	Manipulación no autorizada de los servidores.	Carencia de medios de autenticación para el acceso al Datacenter donde se encuentran los servidores.	Pérdidas financieras por indisponibilidad de las aplicaciones corporativas.
ANS-GI-R11	Aplicación OSTicket	Pérdidas de datos	Ausencia de mecanismos de asignación de usuarios de acceso a la aplicación de gestión de incidentes.	Pérdidas financieras y reputacionales por gestión inadecuada de incidentes derivadas del uso de un mismo usuario por parte de varias personas.
ANS-GI-R12	Personal de Soporte operaciones	Divulgación no autorizada de información sensible o confidencial	Ausencia de mecanismos de validación de cumplimiento de políticas de divulgación de información confidencial o sensible	Pérdidas reputacionales derivadas del manejo inadecuado de información confidencial o sensible por parte del personal de atención de incidentes de clientes.
ANS-GI-R14	Sistema de gestión de red Ubiquiti	Indisponibilidad de servicios por configuraciones inadecuadas o no planeadas de los equipos de red y seguridad.	Ausencia de políticas de asignación de perfiles de acceso a plataforma de configuración de equipos de red.	Pérdidas reputacionales, legales y financieras por indisponibilidad de los servicios.
ANS-GI-R15	Google Drive	Pérdidas de datos sensibles de la empresa	Carencia de políticas de respaldo de la información almacenada en la nube pública.	Pérdidas reputacionales, legales y financieras por indisponibilidad de la información de incidentes de clientes.
ANS-GI-R16	Aplicación OSTicket	Acceso no autorizado a la apertura de incidentes por parte de clientes.	Ausencia de políticas de alta y baja de clientes de la plataforma de gestión de incidentes.	Pérdidas reputacionales y financieras por alteración no autorizada de la información incidentes de clientes.

Tabla 20 Listado de riesgos con nivel elevado riesgo inherente

3.3.2.2 Evaluación de controles

Con base en el análisis de riesgos, realizamos la evaluación de controles basados en la norma NTC-ISO/IEC 27002:2013. Tomando los riesgos con un riesgo inherente elevado, revisamos los controles de la norma que están diseñados para reducir el impacto de las amenazas y vulnerabilidades detectadas sobre el sistema de gestión de la seguridad de la información de ANS Comunicaciones. Se encuentra que los dominios de la norma que involucran riesgos encontrados son los siguientes:

- ✓ Seguridad de los recursos humanos.
- ✓ Control de acceso.
- ✓ Seguridad física y del entorno.
- ✓ Seguridad de las operaciones.
- ✓ Seguridad de las comunicaciones.
- ✓ Gestión de incidentes de seguridad de la información.
- ✓ Cumplimiento.

De los dominios encontrados, se revisaron los controles que aplican a los riesgos que como se mencionó, tienen un elevado riesgo inherente. En total se encontró que 27 controles aplican para disminuir el riesgo. Esos 27 controles se clasifican por su tipo (Preventivo, Detectivo o Correctivo), su clase de implementación (Manual, automática o combinada), su tipo de documentación (No documentado, Documentado no actualizado, Documentado actualizado y documentado desplegado) y finalmente por nivel de percepción de efectividad (Alta, media, poca y ninguna). La relación completa de los controles se encuentra en el Anexo B “Formato matriz de

controles ANS Comunicaciones".

A partir de esta clasificación y analizando los resultados de la misma, encontramos que 6 de los controles requieren ser auditados de manera prioritaria con base en los siguientes criterios:

- ✓ Han sido documentados o documentados desplegados.
- ✓ Su percepción de efectividad es alta o media.
- ✓ Aplica a varios riesgos identificados con riesgo inherente alto.

La relación de los controles a auditar de manera prioritaria se relaciona en la tabla "Controles a auditar en ANS Comunicaciones".

Dominio de control ISO 27002	Código de objetivo de control Norma ISO 27002	Código del Control auditoría	Nombre del control	Descripción del control
Control de acceso	**A.9.1.2**	ANS-PGI-C10	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.9.3.1	ANS-PGI-C12	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
	A.9.4.1	ANS-PGI-C13	Restricción del acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
Seguridad de las operaciones	**A.12.3.1**	ANS-PGI-C19	Respaldo de la información	Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
Seguridad de las comunicaciones	**A.13.2.4**	ANS-PGI-C22	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
	A.13.1.1	ANS-PGI-C24	Controles de las redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

Tabla 21 Controles a auditar en ANS Comunicaciones

3.3.2.3 Generación de guías de auditoría.

Las pruebas de auditoría a realizar al proceso de gestión de incidentes de clientes de ANS Comunicaciones están orientadas a auditar los controles que deben ser auditados de manera inmediata.

Los objetivos de cada una de las pruebas a realizar por parte de la auditoría se encuentran en la tabla “Pruebas de auditoría”.

Nombre de Guía	Objetivos de la prueba	Anexo
Prueba 1	✓ Validar los controles de accesos a redes y aplicaciones. ✓ Verificar que los sistemas de control de acceso a redes cuenten con políticas para la asignación de permisos de ingreso a la red. ✓ Verificar que los perfiles configurados de acceso a la red permitan el acceso de acuerdo al nivel de acceso asignado.	Anexo C " Guía de auditoría 1"
Prueba 2	✓ Verificar que los usuarios cumplan las prácticas para el uso de información secreta. ✓ Verificar la existencia de políticas de manejo de información secreta.	Anexo D "Guía de auditoría 2"
Prueba 3	✓ Validar los controles de accesos a la aplicación OSTicket. ✓ Verificar que los sistemas de control de acceso a la aplicación cuenten con políticas para la asignación de permisos de ingreso a la aplicación. ✓ Verificar que los perfiles configurados de acceso a la aplicación permitan el acceso de acuerdo al nivel asignado.	Anexo E "Guía de auditoría 3"
Prueba 4	✓ Verificar la política de respaldo de la información de gestión de incidentes. ✓ Validar los controles de seguridad aplicados sobre la información respaldada. ✓ Validar la integridad de la información respaldada.	Anexo F "Guía de auditoría 4"
Prueba 5	✓ Verificar la política de divulgación de información confidencial de la empresa. ✓ Validar la efectividad de medios de divulgación de las políticas de confidencialidad en el manejo de la información.	Anexo G "Guía de auditoría 5"
Prueba 6	✓ Verificar la política de separación de redes de la empresa. ✓ Confirmar los controles establecidos para la conexión entre redes de la empresa. ✓ Validar si la plataforma de gestión de redes, permite el monitoreo de los cambios que se realicen sobre los permisos de acceso de los usuarios.	Anexo H "Guía de auditoría 6"

Tabla 22 Guías de auditoría

Las guías de auditoría se realizarán de acuerdo a los recursos tanto de personal como logísticos con lo que cuenten tanto ANS Comunicaciones como la presente auditoría para su realización. Los resultados paso a paso de las pruebas se documentarán en los formatos de pruebas de auditoría relacionados en el punto 3.2.2.4 del presente documento.

3.3.3 Ejecución de pruebas de auditoría.

Con base en las guías de auditoría diseñadas para analizar los controles que deben ser evaluados de manera inmediata.

Las pruebas de auditoría fueron ejecutadas entre los días 3 al 5 de junio de 2.019 y contaron con el apoyo del personal de ANS Comunicaciones, teniendo en cuenta las directrices de la gerencia de operaciones que limitaron la acción de la auditoría a revisar la documentación disponible en el gestor documental de la empresa (aplicación Neogestion) y a ingresar a documentos disponibles.

Algunas de las pruebas no fueron posible ejecutarlas o tuvieron un alcance limitado debido a que la gerencia de operaciones definió que para esta auditoría, se evaluarían las funcionalidades de las aplicaciones sin tener acceso a las cuentas de administración de la aplicación de gestión de incidentes (OSTicket) por encontrarse ejecutando los informes del mes de mayo de 2.019. Esto afecto de manera directa la ejecución de la prueba de auditoría 4, la cual estaba orientada a validar los controles sobre las políticas de respaldo de la aplicación OSTicket.

Cada una de las pruebas ejecutadas se encuentran en los papeles de trabajo que forman parte de los legajos de esta auditoría y que se encuentran dentro de los anexos del presente documento.

La relación de los anexos se encuentra en la tabla “Relación de anexos pruebas de auditoría”.

Nombre de la prueba	Anexo
Prueba 1	Anexo I - Papel de Trabajo - Prueba de auditoría 1
Prueba 2	Anexo J - Papel de Trabajo - Prueba de auditoría 2
Prueba 3	Anexo K - Papel de Trabajo - Prueba de auditoría 3
Prueba 5	Anexo L - Papel de Trabajo - Prueba de auditoría 5
Prueba 6	Anexo M - Papel de Trabajo - Prueba de auditoría 6

Tabla 23 Relación de anexos pruebas de auditoría

3.3.3.1 Hallazgos y no conformidades de las pruebas de auditoría.

A continuación, se relacionan los hallazgos de las pruebas relacionadas en el punto anterior.

3.3.3.1.1 *Hallazgos y no conformidades en control de acceso a redes.*

- ✓ Se detectó que la aplicación de gestión de acceso a redes solo permite dos niveles de acceso a usuario, una con todos los privilegios y la otra con acceso de solo lectura.
- ✓ Se evidencia que la aplicación no realiza un control del nivel de seguridad de las claves de usuario a configurarse.
- ✓ Se evidencia que en las cuentas asignadas a los usuarios de la aplicación solo se está usando un factor de autenticación sin tener habilitado el segundo factor de autenticación disponible en la aplicación.
- ✓ Se observa que dentro de los logs de eventos de la aplicación de gestión de redes no hay eventos que permitan detectar accesos no permitidos a la aplicación.
- ✓ Se evidencia que la aplicación de gestión de redes no permite configurar un tiempo mínimo de inactividad para desloguear al usuario que no ha usado la aplicación por un tiempo prolongado.

3.3.3.1.2 *Hallazgos y no conformidades en control de manejo de información secreta.*

- ✓ Se evidencia que no existe una política de manejo de información secreta o confidencial en ANS Comunicaciones.
- ✓ Se evidencia que el manejo de la información secreta o confidencial por parte del personal de operaciones que gestiona los incidentes de clientes no es el adecuado.

3.3.3.1.3 *Hallazgos y no conformidades en control de acceso a aplicación OSTicket*

- ✓ Se evidencia que ANS Comunicaciones utiliza la aplicación OSTicket no solo para la gestión de incidentes de clientes sino para la gestión de las instalaciones de los servicios.
- ✓ Se encuentra que los perfiles de cualquier usuario de la aplicación permiten observar datos sensibles de los demás usuarios internos de la aplicación.
- ✓ Se evidencia que para los perfiles asignados al personal de gestión de incidentes de clientes no está habilitada la opción de modificar información de los demás usuarios de la aplicación, incluso si pertenecen a su mismo perfil y grupo dentro de la aplicación.
- ✓ Se evidencia que la aplicación OSTicket no realiza un control del nivel de seguridad de las claves de usuario a configurarse.
- ✓ Se evidencia que la aplicación OSTicket no permite configurar un tiempo mínimo de inactividad para desloguear al usuario que no ha usado la aplicación por un tiempo prolongado.

3.3.3.1.4 *Hallazgos y no conformidades en control a política de divulgación de información confidencial.*

- ✓ Se evidencia que no hay una política de divulgación de información confidencial en ANS Comunicaciones.
- ✓ Se encuentra que ANS Comunicaciones ha generado algunas políticas encaminadas a definir la forma como se comunican incidentes y eventos que puedan afectar la seguridad en general de la empresa, pero no se especifican dentro de las mismas el manejo de la divulgación de información confidencial.
- ✓ Se evidencia que la aplicación de gestión documental de ANS Comunicaciones permite asignar tareas y establecer controles para la comunicación de las políticas definidas por la empresa, lo cual facilita la divulgación de las políticas actuales y las que se generen a futuro.

3.3.3.1.5 *Hallazgos y no conformidades en control a política de separación de redes.*

- ✓ Se evidencia que las configuraciones en los equipos de acceso de los canales de internet de la compañía se ajustan a lo acordado entre el responsable de la gestión del servicio en ANS Comunicaciones y el proveedor del servicio.
- ✓ Se evidencia que dentro de las configuraciones de los enrutamientos para el servicio de internet, no hay notaciones que permitan tener claridad sobre la función de dicha ruta.
- ✓ Se observa que las políticas de seguridad de navegación para ANS Comunicaciones están establecidas solo a nivel de puertos TCP/UDP.
- ✓ Se evidencia que el swicthes de Core de ANS Comunicaciones no realiza funciones de

enrutamiento a nivel de capa 3 y que está función a está realizando para todos los segmentos, el equipo de seguridad.

- ✓ Se observa que la configuración de los segmentos de red a nivel de capa 2 tienen correspondencia con los segmentos habilitados por parte de la empresa y que los mismos se encuentran debidamente nominados dentro de las configuraciones tanto de los switches de acceso como de Core.
- ✓ Se evidencia que la navegación de la red Wifi de la sede de ANS Comunicaciones se encuentra controlada hacia las demás redes de la empresa.

3.3.4 Informe de auditoría.

Con base en la ejecución de las pruebas de auditoría y los hallazgos encontrados en las mismas, se dan las siguientes recomendaciones, directrices y acciones a implementar al sistema general de seguridad de la información del proceso de gestión de incidentes de clientes de Networking de ANS Comunicaciones.

Se establece que el sistema general de seguridad de la información del proceso objeto de esta auditoría cuenta con un esquema básico que permite a la empresa ANS Comunicaciones establecer y controlar algunos de los riesgos a los cuales se encuentra expuesta la empresa y puntualmente el proceso de gestión de incidentes.

De primera mano se encuentra que la seguridad de la información se encuentra enmarcada dentro del Sistema de Gestión Integral (SGI) que la empresa ha implementado como parte de las

certificaciones que han adelantado bajo los marcos ISO 9001, ISO 14001 e OHSAS 18001, pero no hay políticas dentro del Sistema de Gestión Integral que permitan establecer la orientación que tiene la empresa sobre la seguridad de la información.

Los controles que fueron tanto evaluados como auditados muestran sin embargo que la empresa cuenta con algunas directrices que se han establecido con base en la experiencia que como compañía del sector de las telecomunicaciones han adquirido a lo largo de más de 20 años de operaciones.

Es de suma importancia para la empresa poder definir un Sistema general de seguridad de la información no solo para el proceso objeto de este estudio, sino para las demás aplicaciones de negocio aprovechando el conocimiento que ya la compañía posee en normas de estandarización como las ISO y las OHSAS.

Las recomendaciones, directrices y acciones a implementar se presentan a continuación:

- ✓ Se recomienda validar con los proveedores de las aplicaciones que hacen parte del proceso de gestión de incidentes las configuraciones o actualizaciones necesarias para definir niveles de acceso diferenciados tanto para los usuarios que administran las plataformas como para los supervisores y operadores y demás usuarios que deban acceder a las mismas.
- ✓ Se recomienda solicitar a los proveedores de las aplicaciones la actualización de las plataformas para permitir mayores niveles de seguridad en las claves de acceso de los usuarios a las plataformas o la implementación de configuraciones o herramientas de segundo factor de autenticación.

- ✓ Se recomienda a ANS Comunicaciones generar políticas de manejo y divulgación de información secreta o confidencial, inicialmente como parte del Sistema de Gestión Integral actualmente implementado.
- ✓ Se recomienda a ANS Comunicaciones separar dentro de la aplicación de gestión de incidentes la gestión de los incidentes de clientes y la gestión de las instalaciones de los servicios, con el fin de segregar los parámetros de medición de acuerdos de niveles de servicios que son diferentes para cada proceso.
- ✓ Se recomienda la implementación de bloqueo automático de los equipos de computo del personal de gestión de incidentes.
- ✓ Se recomienda realizar seguimiento a la notificación y cumplimiento de las diferentes directrices que se generen desde la herramienta de gestión documental a través de la implementación de notificaciones automáticas ante una no respuesta por parte de los empleados a las tareas de notificación que la herramienta genera.
- ✓ Se recomienda al área encargada de la gestión de los contratos de servicios de internet solicitar la configuraciones de las notaciones que permitan diferenciar con claridad cada una de las funciones que realiza los equipos de enrutamiento y de esta forma mejorar las respuestas ante incidentes que se presenten con los servicios.
- ✓ Se recomienda la implementación de políticas de seguridad perimetral basadas en control de aplicaciones y filtrado de contenido, dado que los servicios que actualmente operan en la red de ANS Comunicaciones están orientados a aplicaciones WEB, lo que hace ineficiente el control por puertos TCP/UDP.
- ✓ Se recomienda la implementación de enrutamientos de capa 3 para los segmentos de red corporativos en los swicthes de Core, con el fin de evitar cargas de procesamiento a los

equipos de seguridad perimetral.

- ✓ Es necesario por parte de ANS Comunicaciones la definición de un Sistema de gestión de la seguridad de la información, independiente del sistema de gestión integral que permita implementar las políticas necesarias para proteger los activos de información de una manera eficiente y alineada a los objetivos del negocio.
- ✓ Se hace urgente la capacitación al personal responsable del sistema de gestión integral en temas relacionados con seguridad de la información para que puedan reaccionar de una manera adecuada ante reporte de eventos que puedan comprometer los activos de información. Esto nace de que en la actualidad son ellos los encargados de gestionar los reportes de incidentes de toda índole mientras no se implemente un sistema de gestión de la seguridad de la información.

4. RESULTADOS

- ✓ Se elaboró la auditoría al sistema de gestión de la seguridad de la información del proceso de gestión de incidentes de clientes de Networking de ANS Comunicaciones, usando como base la norma ISO 27002:2013. La auditoría entrego el informe de hallazgos y no conformidades así como las recomendaciones para implementar en el sistema de gestión de la seguridad de la información del proceso auditado.
- ✓ Se realizó la descripción del sistema de información del proceso de gestión de incidentes de ANS Comunicaciones con base en la contextualización realizada tanto de la empresa tanto de los factores externos como internos y la información proporcionada en el marco geográfico.
- ✓ Fueron identificados los requisitos de seguridad para el proceso de gestión de incidentes de ANS Comunicaciones, mediante la evaluación e identificación de riesgos realizada.
- ✓ Los riesgos de la seguridad de la información fueron determinados a través de evaluación de riesgos efectuada, usando como base las directrices de la norma ISO 31000. Esta evaluación permitió la definición de los riesgos así como su evaluación para determinar la prioridad en el tratamiento de los mismos.
- ✓ Se logró diferenciar los dominios de la norma ISO 27002:2013 que son aplicables a los riesgos evaluados en el proceso de gestión de incidentes. Los dominios diferenciados abarcan la seguridad de recursos humanos, las comunicaciones, las operaciones y la seguridad física y del entorno, así como el control de acceso y el cumplimiento.
- ✓ Mediante la diferenciación de los dominios y la evaluación de los riesgos del proceso de

gestión de incidentes, basados en la norma ISO 27002:2013, se seleccionaron los controles a evaluar dentro de la auditoría al sistema de gestión de la seguridad de la información del proceso mencionado.

- ✓ Luego de realizada la auditoría mediante la ejecución de las guías de auditoría diseñadas para evaluar los controles seleccionados de la norma ISO 27002:2013, inferimos las recomendaciones a dar a ANS Comunicaciones para mitigar las amenazas y vulnerabilidades asociadas a los riesgos detectados.
- ✓ Se formulan directrices a desarrollar por parte de ANS Comunicaciones dentro del sistema de gestión de la seguridad de la información. Estas directrices buscan alinear las decisiones de las directivas del negocio en pro de implementar un sistema de gestión de seguridad de la información autónomo y que permita mostrar los activos de información como uno de los pilares de los procesos de negocio de la empresa.
- ✓ Se especifican las acciones tendientes a implementar por parte de ANS Comunicaciones dentro del proceso de gestión de incidentes para mitigar las no conformidades halladas en la auditoría del proceso de gestión de incidentes.
- ✓ Se encuentra que algunas normas como las ISO 9001 e ISO 14001 puedan definir ciertas políticas que ayudan a mitigar amenazas y vulnerabilidades de los activos de información. Pero un sistema de gestión integral no tiene la capacidad de reaccionar de la misma manera que lo hace un sistema de gestión de la seguridad de la información porque sus objetivos son diferentes.

5. CONCLUSIONES Y RECOMENDACIONES

El desarrollo de presente trabajo refleja los conocimientos adquiridos en la especialización en Auditoría de sistemas de información y se basó en la propuesta de auditar, con base en una norma, un proceso dentro de una empresa del sector productivo colombiano.

Las conclusiones que se pueden dar de lo desarrollado dentro del proyecto son las siguientes:

- ✓ La elaboración de una auditoría de sistemas de información nos brinda un diagnóstico del estado de los riesgos a los que está expuesto no solo el sistema de información en sí, sino de los diferentes activos que se relacionan con el sistema de información.
- ✓ La norma ISO 27002:2013 es una guía que nos permite establecer los controles necesarios para mitigar los riesgos a los que está expuesto el sistema de información. Sin embargo, es necesario utilizar normas de evaluación de riesgos que nos permitan definir los niveles de exposición del riesgo para enfocar los esfuerzos de la auditoría en aquellos que tengan un nivel mayor de impacto y probabilidad. Se debe tener en cuenta que en el proyecto desarrollado, los recursos de tiempo, humanos y logísticos fueron limitados y se enfocaron en las tareas prioritarias, como ocurre en las empresas donde las áreas de auditoría son reducidas o inexistentes.
- ✓ El contexto realizado mediante la matriz de riesgos, nos permitió identificar el sistema de información del proceso de gestión de incidentes de ANS Comunicaciones, lo que lo convierte en una herramienta muy importante para la identificación de riesgos.
- ✓ Mediante la evaluación e identificación de riesgos podemos establecer los requisitos de

seguridad de la información del proceso objeto de esta auditoría, lo cual se establece mediante el análisis de amenazas y vulnerabilidades a los que están expuestos los activos del proceso.

- ✓ La evaluación de los riesgos a los que está expuesto el proceso de gestión de incidentes nos permitió identificar el impacto y la probabilidad de ocurrencia de los mismos dando como resultado el cálculo del riesgo inherente, el cual es una valiosa herramienta que permite a las áreas de auditoría y auditores enfocar sus esfuerzos en los procesos y subprocesos que tengan un impacto mayor en el negocio.
- ✓ La evaluación de controles es una herramienta clave para diferenciar los dominios de la norma NTC-ISO 27002:2013, teniendo en cuenta que se debe partir de una correcta evaluación de los riesgos que permita definir los dominios que se van a incluir en una auditoría basada en la norma mencionada anteriormente.
- ✓ Al igual que con la selección de los dominios, la evaluación de controles se requiere para la selección de los controles que se van a incluir dentro del proceso de auditoría. Más allá de su selección, se debe tener en cuenta los criterios que permitan priorizar los esfuerzos de la auditoría y sobre los cuales recaerán las labores iniciales del auditor. En presente proyecto se tuvieron en cuenta su documentación, percepción de efectividad y cobertura a la mayor cantidad de riesgos pero pueden plantearse criterios distintos con base en las necesidades puntuales del negocio y la auditoría.
- ✓ Las recomendaciones que se pueden inferir para las mejoras al sistema de gestión de la seguridad de la información son dependientes del diseño de las guías de auditoría y de la forma en que se realiza su ejecución. Por eso es muy importante que el auditor tenga claridad sobre los objetivos, recursos necesarios y las validaciones que se deben plantear

en una guía de auditoría y que la ejecución de la misma se ciña a las validaciones planteadas.

- ✓ A su vez, las conclusiones que se dan dentro de la prueba de auditoría como resultado de la ejecución de la guía de auditoría, dependen en gran medida del conocimiento y la experiencia del auditor en el proceso evaluado así como en el conocimiento que el mismo tenga del proceso auditado y como este se alinea a los objetivos del negocio.
- ✓ La experiencia que tengan las empresas en certificaciones de la familia ISO puede ser la base para la implementación de un sistema de gestión de la seguridad de la información, teniendo claridad en que los objetivos de cada una de las normas es distinto pero que su fin es gestionar activos, que en el caso analizado en este proyecto fueron los activos de la información.
- ✓ La auditoría debe contar con el apoyo no solo de la dirección de la empresa sino de los responsables y dueños de los procesos auditados, para que la validación diseñada en las guías de auditoria pueda ser llevada a cabo de la manera más efectiva posible en pro de obtener los mejores resultados.
- ✓ Una auditoría de sistemas de información debe contar con personal auditor capacitado en los diferentes componentes que generalmente se pueden encontrar en estos sistemas. El conocimiento no solamente debe cubrir los ámbitos técnicos, necesarios para los procesos tecnológicos, sino que también debe cubrir aspectos de índole financiero, legal, social, económico y todo aquello que se detecte puede llegar a ser útil en la labor de auditoría.

BIBLIOGRAFÍA

ANS Comunicaciones. (2018). Obtenido de www.anscomunicaciones.com.co/ans/nosotros.html

ANS Comunicaciones. (2018). *www.anscomunicaciones.com.co*. Obtenido de http://www.anscomunicaciones.com.co/ans/nosotros.html

Arias Reyes, Y. L., Diaz Rodriguez, M. L., & Vargas Carvajal, J. A. (2014). ELABORACIÓN DE UNA GUÍA DE GESTIÓN DE RIESGOS. *ELABORACIÓN DE UNA GUÍA DE GESTIÓN DE RIESGOS*. Bogotá, Colombia. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/1758/1/Trabajo%20de%20Grado%20Especializacion%20Auditoria%20de%20Sistemas.pdf

Comisión de Regulación Comunicaciones. (2016). *Resolución 5050.* Bogotá.

Comisión de Regulación de Comunicaciones. (2011). *Resolución 3066.* Bogotá.

Comisión de Regulación de Comunicaciones. (2011). *Resolución 3067.* Bogotá.

Comisión de Regulación de Comunicaciones. (2012). *Resolución 3789.* Bogotá.

Comisión de Regulación de Comunicaciones. (2015). *Resolución 4838.* Bogotá.

Congreso. (1994). *Ley 1341.* Bogotá - Colombia.

Congreso. (1994). *Ley 142.* Bogotá - Colombia.

Congreso. (1994). *Ley 143.* Bogotá - Colombia.

IBARRA, J. A., & RICO, S. (31 de 10 de 2013). *ACADEMIA*. Obtenido de https://www.academia.edu/31530752/COBIT_5_for_Risk

Jimenez, F. (2019). *GENIUS IT TRAINING*. Obtenido de geniusitt.com/blog/como-implementar-gestion-de-incidentes-usando-itil/

MINTIC. (2010). *Resolución 202.* Bogotá.

MINTIC. (2013). *Decreto 2044.* Bogotá.

MINTIC. (2014). *Decreto 542.* Bogotá.

MINTIC. (2015). *Decreto1078.* Bogotá.

MINTIC. (2015). *Resolución 917.* Bogotá.

MINTIC. (2016). *Resolución 1260.* Bogotá.

Neira, A. L. (2012). *http://www.iso27000.es/glosario.html#section10a*.

Picón Carrascal, I. (6 de Junio de 2016). Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. *Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*. Bogotá. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/54261/5/ipiconTFM0616memoria.pdf

PMBOK, G. (s.f.). *Tema N° 5 La Estructura de Desglose del Trabajo (EDT) según La Guía del PMBOK® / 30-04-2012 / Sesión 10 segunda parte*. Obtenido de https://formulaproyectosurbanospmipe.wordpress.com

Senado de la República. (1994). *Ley 143 de 1994 Régimen para la generación.* Bogotá.

Anexos

Anexo A. Formato matriz de riesgos ANS Comunicaciones

ANEXOS\FORMATO MATRIZ DE RIESGOS ANS COMUNICACIONES.xlsx

Anexo B. Formato matriz de controles ANS Comunicaciones

ANEXOS\FORMATO MATRIZ DE CONTROLES ANS COMUNICACIONES.xlsx

Anexo C. Guía de auditoría 1

ANEXOS\Guia de auditoría 1.docx

Anexo D. Guía de auditoría 2

ANEXOS\Guia de auditoría 2.docx

Anexo E. Guía de auditoría 3

ANEXOS\Guia de auditoría 3.docx

Anexo F. Guía de auditoría 4

ANEXOS\Guia de auditoría 4.docx

Anexo G. Guía de auditoría 5

ANEXOS\Guia de auditoría 5.docx

Anexo H. Guía de auditoría 6

ANEXOS\Guia de auditoría 6.docx

Anexo I. Papel de Trabajo - Prueba de auditoría 1

ANEXOS\Papel de Trabajo - Prueba de auditoría 1.docx

Anexo J. Papel de Trabajo - Prueba de auditoría 2

ANEXOS\Papel de Trabajo - Prueba de auditoría 2.docx

Anexo K. Papel de Trabajo - Prueba de auditoría 3

ANEXOS\Papel de Trabajo - Prueba de auditoría 3.docx

Anexo L. Papel de Trabajo - Prueba de auditoría 5

ANEXOS\Papel de Trabajo - Prueba de auditoría 5.docx

Anexo M. Papel de Trabajo - Prueba de auditoría 6

ANEXOS\Papel de Trabajo - Prueba de auditoría 6.docx